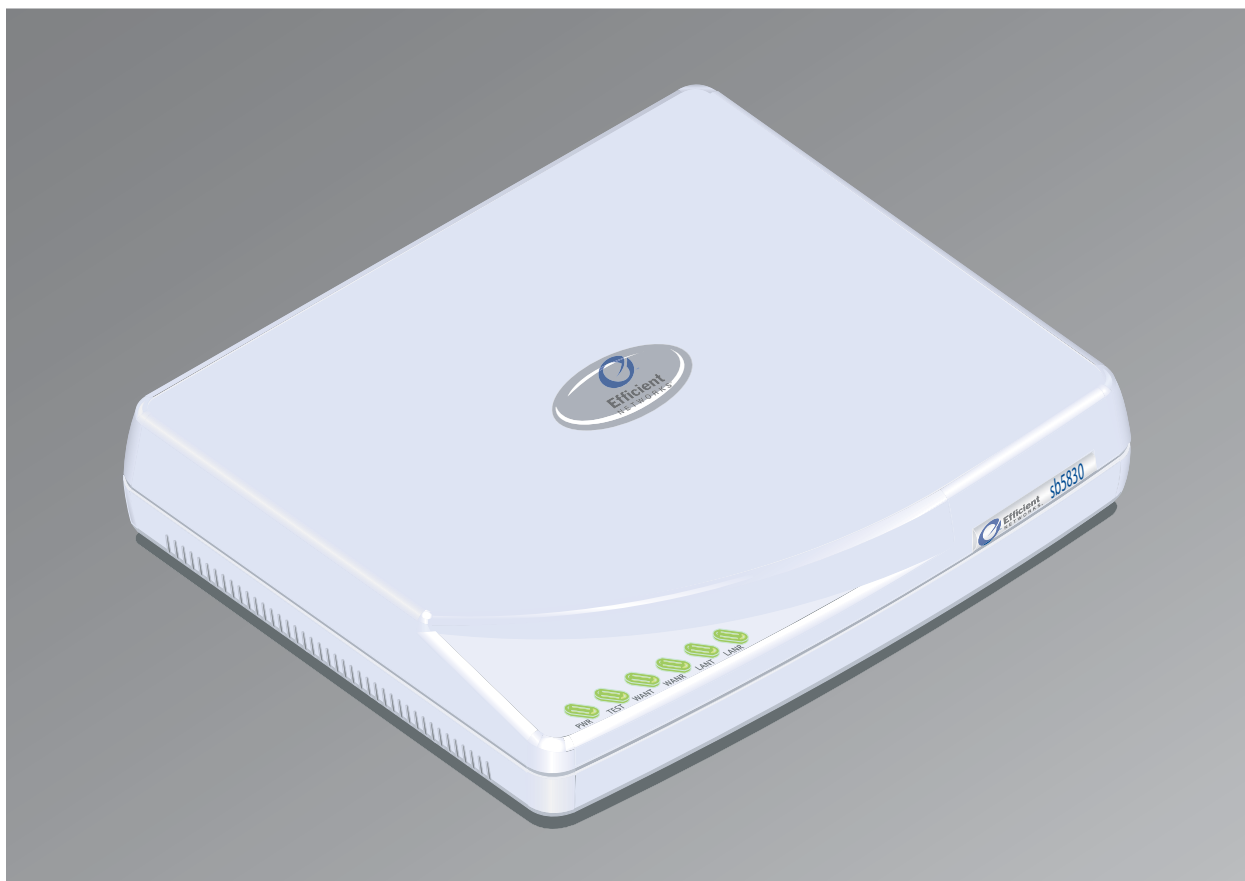




sb5830 & sb5835

Broadband Internet Router



Gebruikershandboek

Efficient Networks and SpeedStream are registered trademarks, and the Efficient Networks logo is a trademark of Efficient Networks, Inc. All other names may be trademarks, service marks or registered trademarks held by their respective companies. This document is for information purposes only, Efficient Networks is not responsible for errors or omissions herein. Efficient reserves the right to make changes to product specifications without notice.

Efficient Networks, Inc. – End User Software License and Warranty

INSTALLATION OF THE HARDWARE AND SOFTWARE PROVIDED BY EFFICIENT NETWORKS, INC. ("EFFICIENT") CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS OF THE FOLLOWING SOFTWARE LICENSE AND LIMITED WARRANTY. IF YOU DO NOT ACCEPT THESE TERMS, PLEASE RETURN THE HARDWARE AND SOFTWARE AND SOFTWARE IN ITS ORIGINAL PACKAGING TO THE VENDOR FROM WHICH YOU PURCHASED IT FOR A FULL REFUND OF THE PURCHASE PRICE.

The following describes your license to use the software (the "Software") that has been provided with your EFFICIENT DSL customer premise equipment ("Hardware") and the limited warranty that EFFICIENT provides on its Software and Hardware. EFFICIENT reserves any right not expressly granted to the end user.

Software License

The Software is protected by copyright laws and international copyright treaties. The Software is licensed and not sold to you. The definition of Software includes, but not limited to, system and operating software marketed by EFFICIENT, including firmware, embedded software, software provided on media, downloadable software, software for configuration or programmable logic elements, and all EFFICIENT maintenance and diagnostic tools associated with the above mentioned software. Accordingly, while you own the media (such as CD ROM or floppy disk) on which the software is recorded, EFFICIENT or its licensors retains ownership of the Software itself.

1. **Grant of License.** You may install and use one (and only one) copy of the Software in conjunction with the EFFICIENT provided Hardware. You may make backup copies of the system configuration as required. If the Hardware is being installed on a network, you may install the Software on the network server or other server-side device on which the Hardware is being installed and onto the client-side devices.
2. **Restrictions.** The license granted is a limited license. You may NOT:
 - sublicense, assign, or distribute copies of the Software to others;
 - decompile, reverse engineer, disassemble or otherwise reduce the Software or any part thereof to a human perceivable form;
 - modify, adapt, translate or create derivative works based upon the Software or any part thereof; or
 - rent, lease, loan or otherwise operate for profit the Software.
3. **Transfer.** You may transfer the Software only where you are also transferring the Hardware. In such cases, you must remove all copies of the Software from any devices onto which you have installed it, and must ensure that the party to whom you transfer the Hardware receives this License Agreement and Limited Warranty.
4. **Upgrades Covered.** This License covers the Software originally provided to you with the Hardware, and any additional software that you may receive from EFFICIENT, whether delivered via tangible media (CD ROM or floppy disk), downloaded from EFFICIENT, or delivered through customer support. Any such additional software shall be considered "Software" for all purposes under this License.
5. **Export Law Assurances.** You acknowledge that the Software may be subject to export control laws and regulations of the U.S.A. You confirm that you will not export or re-export the Software to any countries that are subject to export restrictions.
6. **No Other Rights Granted.** Other than the limited license expressly granted herein, no license, whether express or implied, by estoppel or otherwise, is granted to any copyright, patent, trademark, trade secret, or other proprietary rights of EFFICIENT or its licensors.
7. **Termination.** Without limiting EFFICIENT's other rights, EFFICIENT may terminate this license if you fail to comply with any of these provisions. Upon termination, you must return the Software and all copies thereof.

Limited Warranty

The following limited warranties provided by EFFICIENT extend to the original end user of the Hardware/licensee of the Software and are not assignable or transferable to any subsequent purchaser/licensee.

1. **Hardware.** EFFICIENT warrants that the Hardware will be free from defects in materials and workmanship and will perform substantially in compliance with the user documentation relating to the Hardware for a period of one year from the date the original end user received the Hardware.
2. **Software.** EFFICIENT warrants that the Software will perform substantially in compliance with the end user documentation provided with the Hardware and Software for a period of ninety days from the date the original end user received the Hardware and Software. The end user is responsible for the selection of Hardware and Software used in the end user's network. Given the wide range of third-party hardware and applications, EFFICIENT does not warrant the compatibility or uninterrupted or error free operation of our Software with the end

user's systems or network.

3. **Exclusive Remedy.** Your exclusive remedy and EFFICIENT's exclusive obligation for breach of this limited warranty is, in EFFICIENT's sole option, either (a) a refund of the purchase price paid for the Hardware/Software or (b) repair or replacement of the Hardware/Software with new or remanufactured products. Any replacement Hardware or Software will be warranted for the remainder of the original warranty period or thirty days, whichever is longer.

4. **Warranty Procedures.** If a problem develops during the limited warranty period, the end user shall follow the procedure outlined below:

A. Prior to returning a product under this warranty, the end user must first call EFFICIENT at (888) 286-9375, or send an email to EFFICIENT at support@efficient.com to obtain a return materials authorization (RMA) number. RMAs are issued between 8:00 a.m. and 5:00 p.m. Central Time, excluding weekends and holidays. The end user must provide the serial number(s) of the products in order to obtain an RMA.

B. After receiving an RMA, the end user shall ship the product or defective component, including power supplies and cable, where applicable, freight or postage prepaid and insured, to EFFICIENT at 4849 Alpha Road, Dallas Texas 75244, U.S.A. Within five (5) days notice from EFFICIENT, the end user shall provide EFFICIENT with any missing items or, at EFFICIENT's sole option, EFFICIENT will either (a) replace missing items and charge the end user or (b) return the product to the end user freight collect. The end user shall include a return address, daytime phone number and/or fax. The RMA number must be clearly marked on the outside of the package.

C. Returned Products will be tested upon receipt by EFFICIENT. Products that pass all functional tests will be returned to the end user.

D. EFFICIENT will return the repaired or replacement Product to the end user at the address provided by the end user at EFFICIENT Network's expense. For Products shipped within the United States of America, EFFICIENT will use reasonable efforts to ensure delivery within five (5) business days from the date received by EFFICIENT. Expedited service is available at additional cost to the end user.

E. Upon request from EFFICIENT, the end user must prove the date of the original purchase of the product by a dated bill of sale or dated itemized receipt.

5. **Limitations.**

- The end user shall have no coverage or benefits under this limited warranty if the product has been subject to abnormal use, abnormal conditions, improper storage, exposure to moisture or dampness, unauthorized modifications, unauthorized repair, misuse, neglect, abuse, accident, alteration, improper installation, or other acts which are not the fault of EFFICIENT, including acts of nature and damage caused by shipping.
- EFFICIENT will not honor, and will not consider the warranty voided, if: (1) the seal or serial number on the Product have been tampered with or (2) there has been any attempted or actual repair or modification of the Product by anyone other than an EFFICIENT authorized service provider.
- The limited warranty does not cover defects in appearance, cosmetic, decorative or structural items, including framing, and any non-operative parts.
- EFFICIENT's limit of liability under the limited warranty shall be the actual cash value of the product at the time the end user returns the product for repair, determined by the price paid by the end user for the product less a reasonable amount for usage. EFFICIENT shall not be liable for any other losses or damages.
- The end user will be billed for any parts or labor charges not covered by this limited warranty. The end user will be responsible for any expenses related to reinstallation of the product.
- THIS LIMITED WARRANTY IS THE ONLY WARRANTY EFFICIENT MAKES FOR THE PRODUCT AND SOFTWARE. TO THE EXTENT ALLOWED BY LAW, NO OTHER WARRANTY APPLIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

6. **Out of Warranty Repair.** Out of warranty repair is available for a fixed fee. Please contact EFFICIENT at the numbers provided above to determine out of warranty repair rate. End users seeking out of warranty repair should contact EFFICIENT as described above to obtain an RMA and to arrange for payment of the repair charge. All shipping charges will be billed to the end-user.

General Provisions

The following general provisions apply to the foregoing Software License and Limited Warranty.

1. **No Modification.** The foregoing Limited Warranty is the end user's sole and exclusive remedy and is in lieu of all other warranties, express or implied. No oral or written information or advice given by EFFICIENT or its dealers, distributors, employees or agents shall in any way extend, modify or add to the foregoing Software License and Limited Warranty. This Software License and Limited Warranty constitutes the entire agreement between EFFICIENT and the end user, and supersedes all prior and contemporaneous representation, agreements or understandings, oral or written. This Software License and Limited Warranty may not be changed or amended except by a written instrument executed by a duly authorized officer of EFFICIENT.

EFFICIENT neither assumes nor authorizes any authorized service center or any other person or entity to assume for it any other obligation or liability beyond that which is expressly provided for in this Limited Warranty including the provider or seller of any extended warranty or service agreement.

The Limited Warranty period for EFFICIENT supplied attachments and accessories is specifically defined within their own warranty cards and packaging.

2. **EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND OTHER DAMAGES.** TO THE FULL EXTENT PERMITTED BY LAW, IN NO EVENT SHALL EFFICIENT OR ITS LICENSORS BE LIABLE, WHETHER UNDER CONTRACT, WARRANTY, TORT OR ANY OTHER THEORY OF LAW FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, PERSONAL INJURY, LOSS OR IMPAIRMENT OF DATA OR BUSINESS INFORMATION, EVEN IF EFFICIENT HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES. EFFICIENT'S OR ITS LICENSOR'S LIABILITY TO YOU (IF ANY) FOR ACTUAL DIRECT DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION, WILL BE LIMITED TO, AND SHALL NOT EXCEED, THE AMOUNT PAID FOR THE HARDWARE/SOFTWARE.

3. **General.** This Software License and Limited Warranty will be covered by and construed in accordance with the laws of the State of Texas, United States (excluding conflicts of laws rules), and shall insure to the benefit of EFFICIENT and its successor, assignees and legal representatives. If any provision of this Software License and Limited Warranty is held by a court of competent jurisdiction to be a invalid or unenforceable to any extent under applicable law, that provision will be enforced to the maximum extent permissible, and the remaining provisions of this Software License and Limited Warranty will remain in full force and effect. Any notices or other communications to be sent to EFFICIENT must be mailed by certified mail to the following address:

Efficient Networks, Inc.
4849 Alpha Road
Dallas, TX 75244
U.S.A.
Attn: Customer Service

INSTALLATIE.....	7
Introductie.....	7
Installatievereisten.....	7
Inhoud van het pakket.....	7
Hardwarevereisten.....	7
Eisen aan uw netwerkprovider.....	7
Sluit u uw router aan.....	8
Configuratie.....	8
Microsoft Windows.....	9
Windows 98.....	9
Windows NT 4.....	10
Windows 2000.....	12
Windows ME.....	14
Windows XP.....	15
Apple Macintosh.....	17
Mac OS 9.x.....	17
Mac OS X.....	18
Linux.....	19
EASY SETUP.....	21
Router Information-scherm.....	21
WAN Interface-scherm.....	22
Point-to-Point Protocol via ATM.....	23
Point-to-Point Protocol via Ethernet via PPPoA.....	24
Point-to-Point Protocol via Ethernet via RFC 1483.....	25
RFC 1483 Networking.....	26
RFC 1483 MAC Encapsulated Routing.....	27
Dynamic Host Configuration Protocol.....	28
Configuratie van een Local Area Network.....	29
Restarting Router-scherm.....	30
GEAVANCEERDE FACILITEITEN.....	31
Access Control.....	32
User Management.....	33
User Management-scherm.....	33
Een nieuwe User Account toevoegen.....	34
User Templates.....	35
Hoe wijzigt u een User Account?.....	35
Hoe verwijdert u een User Account?.....	35
User Lookup Configuration.....	36
Secure Mode Configuration.....	37
Current Date and Time.....	38
DHCP Configuration.....	39
Network Address Translation.....	41
Outbound NAT Setting.....	41
NAT Passthrough Setting.....	42
Inbound NAT Setting.....	42
Easy Setup.....	42
Advanced Setup.....	42
Simple Network Management Protocol (SNMP).....	43
SNMP Configuration-scherm.....	43
SNMP IP Filter.....	44
SNMP Password.....	45
Secure Shell (SSH).....	46
Configureer de Secure Shell (SSH).....	47
Load Public and Private Keys.....	48
Key Generator.....	48
Key Generator Status.....	50
Firewall Configuration.....	51
Quality of Service.....	53
QoS Configuration-scherm.....	53

QoS Policy Configuration	54
Maak of wijzig een QoS Policy	55
Een QoS Policy verschuiven	56
Verwijder een QoS Policy	57
Fris de QoS Policy Configuration op	57
Stateful Firewall	58
Stateful Firewall Configuration-scherm	58
Dropped Packet List	59
Stateful Firewall Rule-configuratie	60
Stateful Firewall Rules maken	61
Wijzig/Bekijk Stateful Firewall Rules	62
Stateful Firewall Rules verwijderen	63
Actualiseer Stateful Firewall Rules	64
Dial Backup	65
ATM Traffic Shaping Configuration	67
Diagnostic	68
Command Line Interface	69
File Editor	70
IKE/IPSec Configuration	71
Easy IKE/IPSec Setup	71
Advanced IKE/IPSec Configuration	72
IKE Peer Definition	73
IKE Proposal Definition	74
IKE IPSec Proposal Definition	75
IKE IPSec Policy Definition	77
SPECIFICATIE	79
Voorzijde	79
Achterzijde	80
Hardwarespecificatie	80
Fysieke specificatie	80
Operationele omgeving	80
Voedingseisen	80
Processor	80
LAN Interface	81
WAN Interface	81
Seriële interface	81
Keuringseisen	81
Softwarespecificatie	81
Bridging	81
Routing	81
Configuratiemanagement	81
Diverse diensten - Quality of Service Provisioning	81
Dial Backup	82
Asynchronous Transfer Mode (ATM)	82
IP Address Translation	82
Protocol-conformiteitstest	82
PPP (RFC 1661)	82
Veiligheid	82
SUPPORT	83

Introductie

Dit gebruikershandboek omvat de installatie en setup van de Efficient Networks sb5830-sb5835 Broadband Internet Router. Het bevat ook specificaties en support-informatie. Dit hoofdstuk begeleidt u door de installatie van uw router.

Installatievereisten

Inhoud van het pakket

Uw routerpakket dient de onderstaande items te bevatten. Als u ziet dat er iets beschadigd is of ontbreekt, neem dan contact op met uw dealer.

- Een Efficient Networks sb5830-sb5835 Broadband Internet Router
- Een cd-rom met documentatie
- Een AC-stroomvoorzieningsmodule met kabel
- Twee RJ-45 Ethernet-kabels
- Een RJ-45/DB-9 seriële poortadapter (console)
- sb5830-sb5835 Broadband Internet Router Customer Release Notes
- sb5830-sb5835 Broadband Internet Router Quick Start Guide

Hardwarevereisten

Uw pc moet zijn toegerust met de volgende hard- en software:

- CD-ROM-station
- Ethernet netwerk-interfacekaart
- TCP/IP netwerkprotocol geïnstalleerd en geactiveerd
- Webbrowser
- Gebruik de terminal emulation software als u de router via de seriële poort van uw eigen pc wilt configureren vóór u de router binnen een netwerk in bedrijf stelt.

Eisen aan uw netwerkprovider

Uw netwerkprovider moet u van specifieke informatie voorzien zodat u uw Efficient Networks sb5830-sb5835 Broadband Internet Router kunt configureren. U hebt de volgende informatie nodig om uw router met succes te kunnen configureren:

- DNS-adres
- Een of meerdere LAN IP-adressen en een subnetmasker
- Kies voor het protocol dat u wilt gebruiken, uit de volgende opties:
- PPP (Point-to-Point Protocol), met een gebruikersnaam en een wachtwoord
- PPPoE (PPP via Ethernet)
- Point-to-Point Protocol via Ethernet via RFC 1483
- RFC 1483 (SNAP Encapsulation)
- RFC 1483 MER (MAC Encapsulated Routing, vereist een WAN gateway-adres)
- VCI (PVC)-nummers
- Network options:
- Bridging
- IP-routing (vereist een WAN IP-adres en een subnetmasker)

Sluit u uw router aan

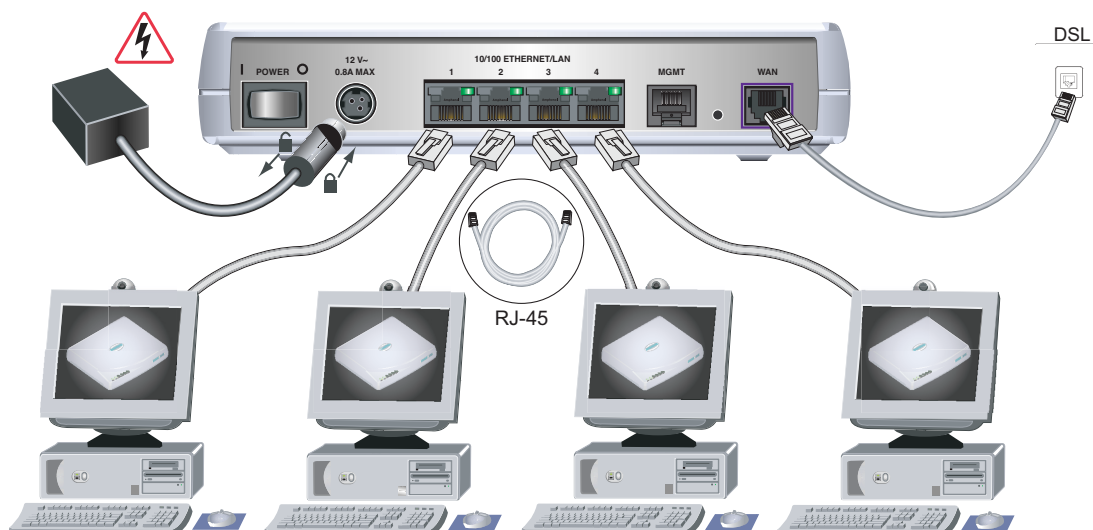
In de volgende procedure wordt beschreven hoe u de kabels op de juiste wijze met uw router moet verbinden.

- Stap 1:** Plaats uw router in een goed geventileerde ruimte. Sluit het niet op andere toestellen aan en plaats het niet op vloerbedekking of een tapijt.
- Stap 2:** Maak een directe verbinding van uw pc met een van de Ethernet-poorten van uw router met behulp van een van de rode kabels. U kunt nog meer Ethernet-apparaten op de resterende Ethernet-poorten aansluiten.
- Stap 3:** Sluit uw router aan op de DSL-bus met behulp van de resterende RJ-45 kabel.
- Stap 4:** Sluit uw router aan op een AC-voeding met behulp van de meegeleverde voedingsadapter en kabel.



PAS OP! Gebruik alleen 26 AWG of sterkere draden (bijv. 24, 22, 20 etc.) ter vermindering van brandgevaar om uw DSL-poort aan uw eenheid aan te kunnen sluiten met een RJ-45-stekker en voor de dial backup-verbinding.

Scherf 1: Aansluiting van de sb5830 routerkabels



Configuratie

Uw computer moet gebruik maken van het TCP/IP-protocol voor de toegang tot internet en DHCP-adres-toekenningen accepteren van uw router. Hoewel de informatie voor zulke instellingen standaard is, gaan de diverse besturingssystemen voor pc's met dit soort instellingen heel verschillend om. Dit gedeelte voorziet in de schermen voor de configuratie van het TCP/IP en DHCP in de gangbare besturingssystemen, die u door de configuratieprocedures binnen elk systeem zullen leiden.

U kunt ook direct kiezen en naar een van de volgende besturingssystemen springen:

- Microsoft Windows
- [Windows 98](#)
- [Windows NT 4](#)
- [Windows 2000](#)

- [Windows ME](#)
- [Windows XP](#)
- Apple Macintosh
- [Mac OS 9.x](#)
- [Mac OS X](#)
- [Linux](#)

Microsoft Windows

Windows 98

Stap 1: Rechtsklik op het pictogram Network Neighborhood op uw bureaublad.

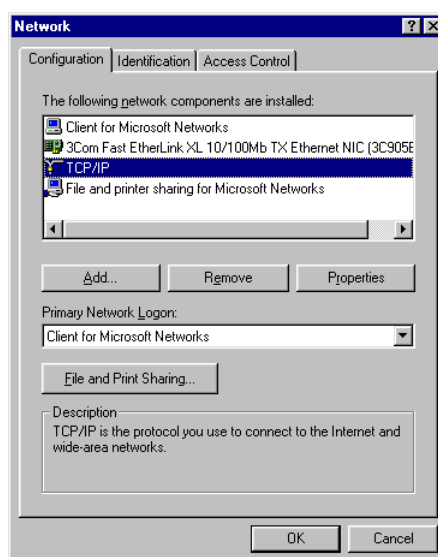
Scherf 2: Het pictogram Network Neighborhood



Stap 2: Nu moet het Network-venster verschijnen. Kies het TCP/IP uit de geïnstalleerde netwerkcomponenten in het tabblad Configuration .

Stap 3: Klik op Properties om de eigenschappen van TCP/IP weer te geven.

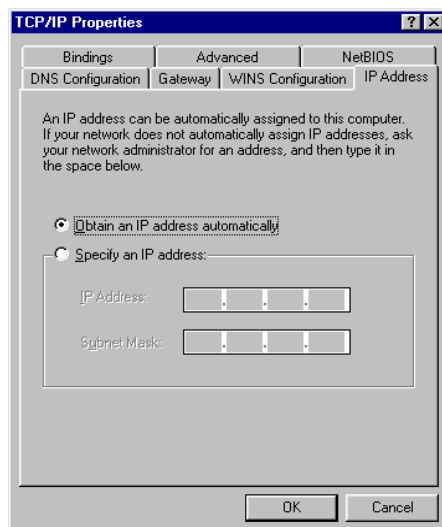
Scherf 3: Het venster Network



Stap 4: Kies het tabblad IP Address in het venster TCP/IP Properties.

Stap 5: Klik in het tabblad IP Address op de optie Obtain an IP address automatically.

Scherf 4: Het venster IP Address



Stap 6: Klik op OK.

Stap 7: Klik op de OK-knoppen om de vensters te sluiten.

Opmerking: Misschien moet u uw pc herstarten zodat de wijzigingen van kracht worden.

Windows NT 4

Stap 1: Rechtsklik op het pictogram Network Neighborhood op uw bureaublad.

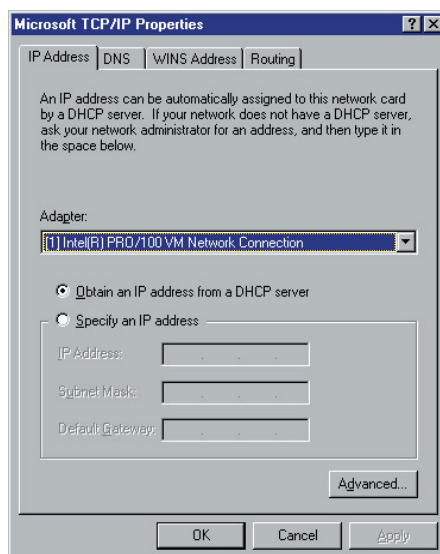
Scherf 5: Het pictogram Network Neighborhood



Stap 2: Nu moet het Network-venster verschijnen. Kies het TCP/IP-protocol in het tabblad Protocols uit de lijst van geïnstalleerde protocollen.

Stap 3: Klik op Properties om de eigenschappen van TCP/IP weer te geven.

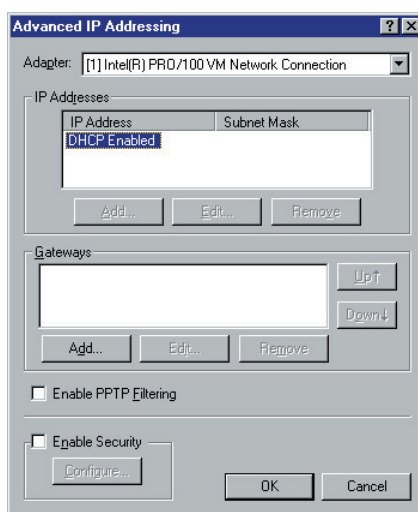
Scherf 6: Het venster TCP/IP Properties



Stap 4: Kies het tabblad IP-adres in het Microsoft-venster TCP/IP-instellingen.

Stap 5: Klik in het tabblad IP Address op de optie Obtain an IP address from a DHCP server.

Scherf 7: Het venster IP Address



Stap 6: Klik op OK.

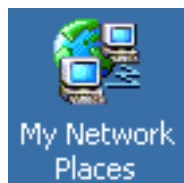
Stap 7: Klik op de OK-knoppen om de vensters te sluiten.

Opmerking: Misschien moet u uw pc herstarten zodat de wijzigingen van kracht worden.

Windows 2000

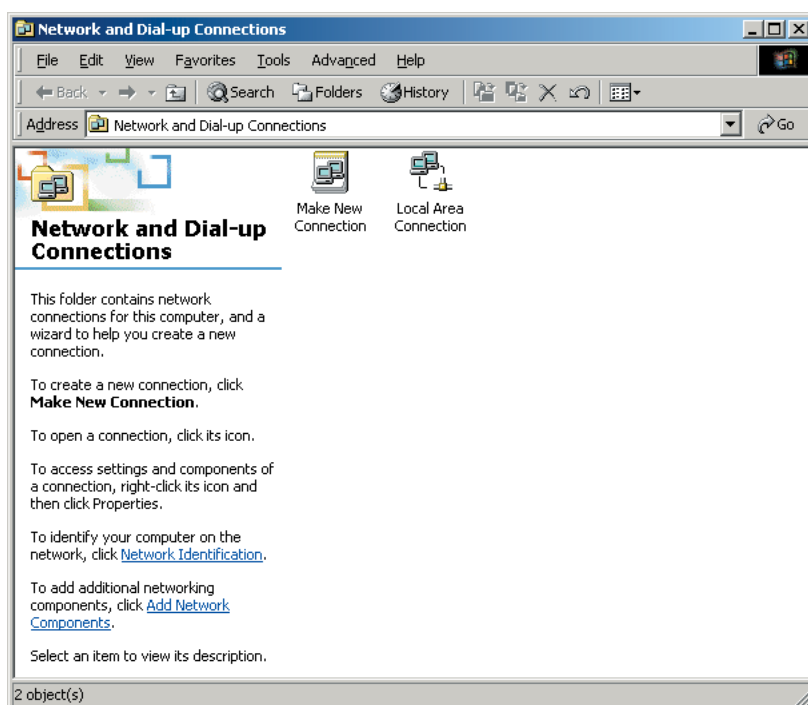
Stap 1: Rechtsklik op het pictogram My Network Places op uw bureaublad.

Scherf 8: Het pictogram My Network Places



Stap 2: Het venster The Network and Dial-up Connections verschijnt. Rechtsklik op het pictogram van de Local Area Connection.

Scherf 9: Network and Dial-Up Connections-venster

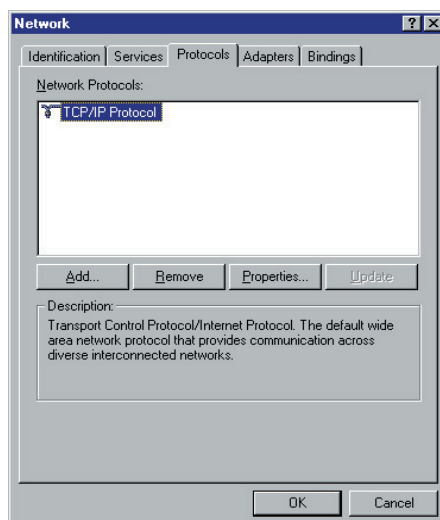


Stap 3: Kies de optie Properties in het menu.

Stap 4: Nu moet het venster Local Area Connection Properties verschijnen. Kies Internet Protocol (TCP/IP) uit de lijst met componenten.

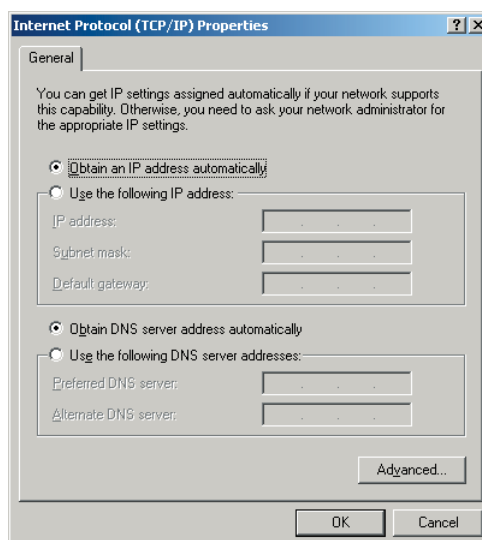
Stap 5: Klik op Properties om de eigenschappen van TCP/IP weer te geven.

Scherf 10: Het venster LAN Properties



Stap 6: Het venster van het Internet Protocol (TCP/IP) Properties verschijnt. Klik op de optie Obtain an IP address automatically en Obtain DNS server address automatically.

Scherf 11: Het venster TCP/IP Properties



Stap 7: Klik op OK.

Stap 8: Klik op de OK-knoppen om de vensters te sluiten.

Opmerking: Misschien moet u uw pc herstarten zodat de wijzigingen van kracht worden.

Windows ME

Stap 1: Rechtsklik op het pictogram Network Places op uw bureaublad.

Scherf 12: Het pictogram Network Places



Stap 2: Kies de optie Properties in het getoonde menu.

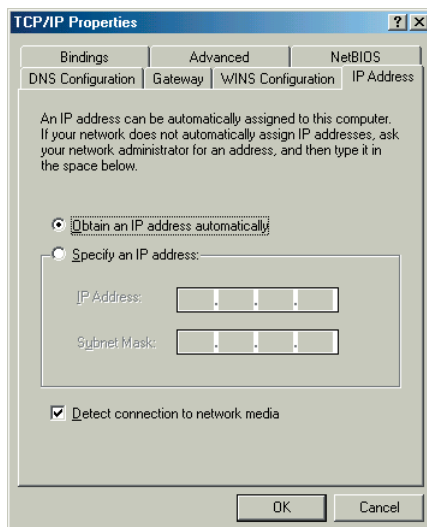
Stap 3: Nu moet het Network-venster verschijnen. Kies in het tabblad Configuration uit de lijst van geïnstalleerde netwerkcomponenten het TCP/IP Protocol dat correspondeert met uw netwerkkaart.

Stap 4: Klik op Properties om de eigenschappen van TCP/IP weer te geven.

Stap 5: Kies het tabblad IP Address in het venster TCP/IP Properties.

Stap 6: Klik in het tabblad IP Address op de optie Obtain an IP address automatically.

Scherf 13: Het venster TCP/IP Properties



Stap 7: Klik op OK.

Stap 8: Klik op de OK-knoppen om de vensters te sluiten.

Opmerking: Misschien moet u uw pc herstarten zodat de wijzigingen van kracht worden.

Windows XP

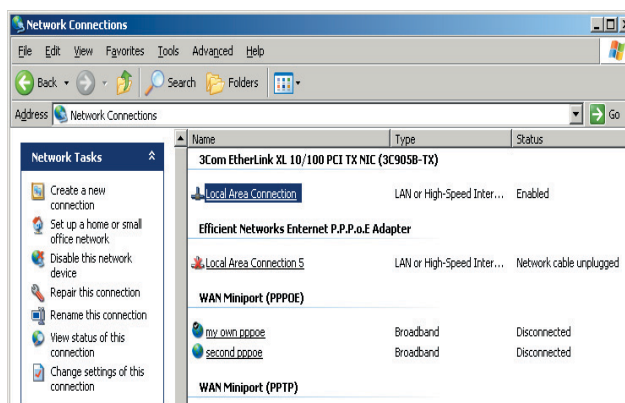
Stap 1: Rechtsklik op het pictogram My Network Places op uw bureaublad.

Scherf 14: Het pictogram My Network Places



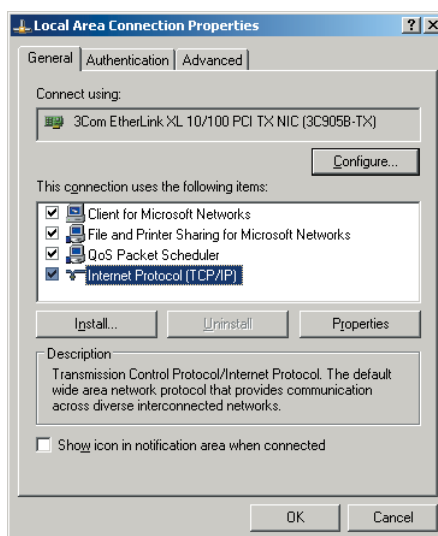
Stap 2: Het scherm My Network Places verschijnt. Kies View Network Connections in het menu Network Tasks.

Scherf 15: Het venster Network Connections



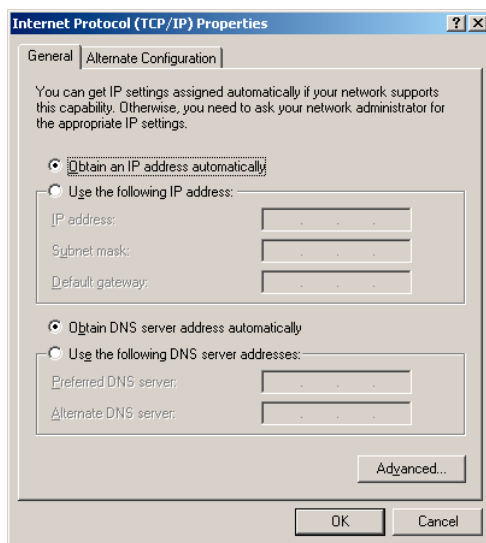
Stap 3: Het scherm Network Connections verschijnt. Klik op het pictogram van de Local Area Connection.

Scherf 16: Het venster LAN Properties



- Stap 4:** Nu moet het venster Local Area Connection Properties verschijnen. Kies het Internet Protocol (TCP/IP) uit de lijst van items.

Scherf 17: Het venster TCP/IP Properties



- Stap 5:** Het venster van het Internet Protocol (TCP/IP) Properties verschijnt. Kies in het tabblad General de opties Obtain an IP address automatically en Obtain DNS server address automatically.

- Stap 6:** Klik op de OK-knoppen om de vensters te sluiten.

Opmerking: Misschien moet u uw pc herstarten zodat de wijzigingen van kracht worden.

Apple Macintosh

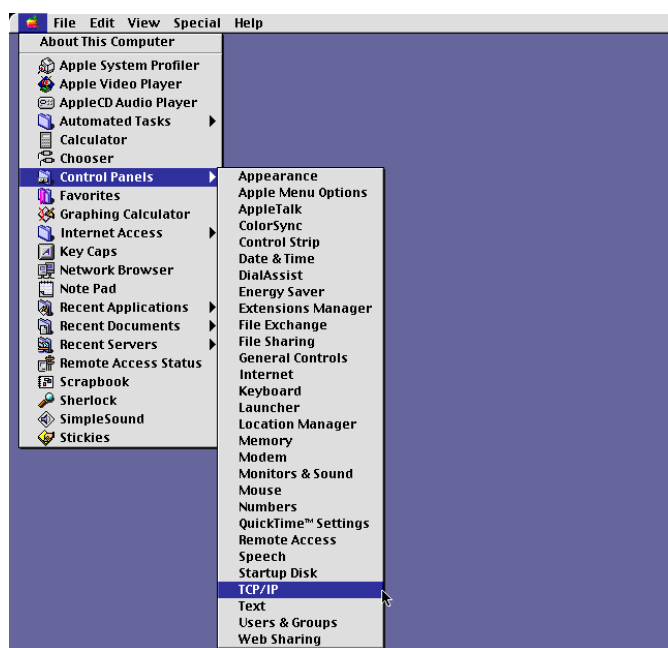
Om TCP/IP en DHCP op uw Macintosh te configureren, moet u eerst de versie van uw Mac OS kiezen:

- [Mac OS 9.x](#)
- [Mac OS X](#)

Mac OS 9.x

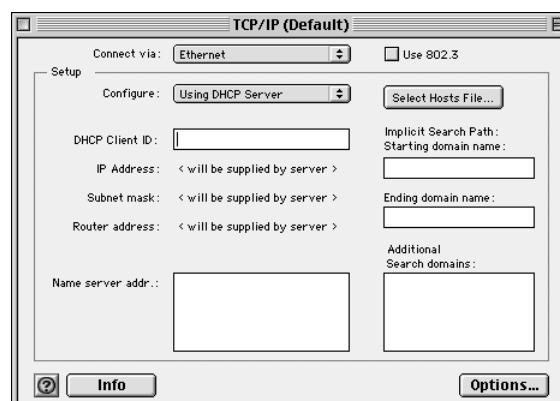
Stap 1: Kies in het Apple-menu de optie Control Panels en vervolgens het TCP/IP.

Scherf 18: Apple Macintosh Control Panels Menu



Stap 2: Het TCP/IP-bedienpaneel verschijnt. Kies Using a DHCP Server uit het meerkeuzemenu Configure.

Scherf 19: TCP/IP bedienpaneel



Stap 3: Vul de velden in met de informatie die u van uw serviceprovider hebt ontvangen.

Stap 4: Klik op het vierkantje helemaal links boven aan in dit venster om het controlepaneel van TCP/IP te sluiten.

Mac OS X

Stap 1: Kies Systeemvoorkeuren in het Apple-menu.

Scherf 20: Apple Macintosh Preferences Menu



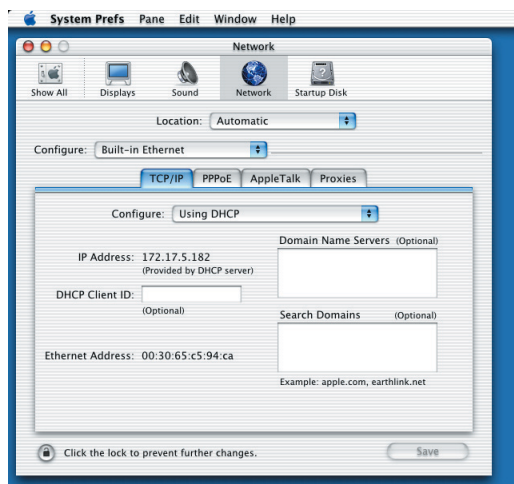
Stap 2: Het venster met de Systeemvoorkeuren verschijnt. Klik om het pictogram Network te kiezen.

Scherf 21: Apple Macintosh Systeemvoorkeuren-venster



Stap 3: Het Netwerk-venster verschijnt. Kies het tabblad TCP/IP.

Scherf 22: Apple Macintosh Netwerk-venster



Stap 4: Kies Using a DHCP Server in het meerkeuzemenu Configure.

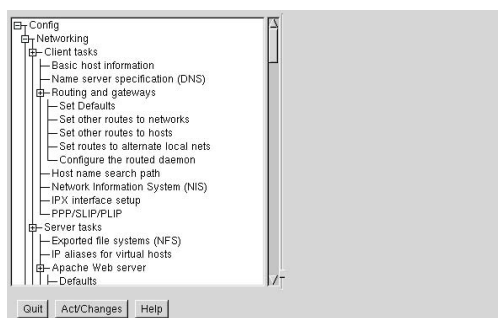
Stap 5: Voer de informatie in die u van uw serviceprovider hebt ontvangen.

Stap 6: Klik op de knop Save om uw instellingen op te slaan en het Netwerk-venster te sluiten.

Linux

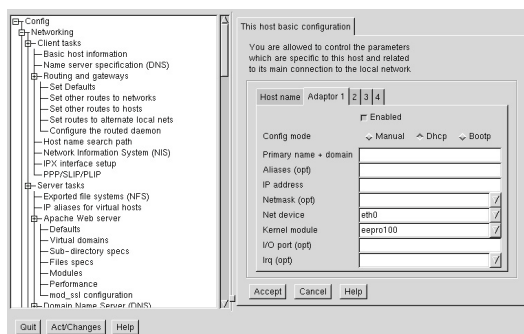
Stap 1: Voer het volgende commando uit via een terminalvenster. `linuxconfig`

Scherf 23: Linux Configuration-scherf



Stap 2: Het Config-venster verschijnt. Voer de informatie in die u van uw serviceprovider hebt ontvangen, in de velden onder het betreffende tabblad.

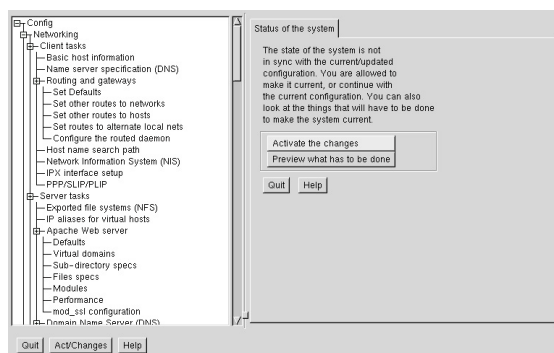
Scherf 24: Linux Host configuratiescherf



Stap 3: Klik op Accept, zodra de instellingen volledig zijn.

Stap 4: Om de systeemstatus te updaten, moet de knop 'Activate the changes' branden; klik vervolgens op Act/Changes.

Scherf 25: Linux Config System Status-scherf



De Easy Setup-schermen zijn gemaakt voor een eenvoudige, stap-voor-stap configuratie van de basisfaciliteiten van de router. Easy Setup bestaat uit webvensters met alle bedienopties voor de setup en het gebruik van uw router. U hebt informatie over uw netwerk nodig om Easy Setup uit te kunnen voeren. Deze informatie krijgt u normaliter van uw netwerkprovider.

De volgende Easy Setup-procedure veronderstelt dat u de vereiste verbindingen tot stand hebt gebracht en bent aangemeld bij de router volgens de beschrijving in de Quick Start Guide. U kunt uw router ook vanaf de prompt met behulp van de Command Line Interface.

Router Information-scherm

Het eerste scherm in de Web User Interface is het Router Information-scherm. Dit scherm toont de basisinformatie en configuratie-instellingen van uw router. Het voorziet ook in links met andere setup- en controlesjablonen van de router. Op het Router Information-scherm is de volgende informatie te zien:

- Router Information - inclusief het modelnummer, het softwareversienummer en de opties die zijn geactiveerd.
- Router Configuration - Toont details van de routerconfiguratie, zoals LAN IP-adres, WAN data en spraak-PVC (ATM), WAN-protocol en WAN-netwerkinstellingen.

In de volgende afbeelding ziet u het scherm van de Router Information.

Scherm 26: Router Information-scherm

Efficient NETWORKS

Current User: superuser

- [Easy Setup](#)
- [Remote File Configuration](#)
- [Change Password](#)
- [Access Control](#)
- [User Management](#)
- [Router Clock](#)
- [DHCP](#)
- [NAT](#)
- [SNMP](#)
- [Secure Shell \(SSH\)](#)
- [Firewall Scripts](#)
- [QoS](#)
- [Stateful Firewall](#)
- [Routing Table Configuration](#)
- [Dial Backup](#)
- [ATM Traffic Shaping](#)
- [Switch Management](#)
- [Diagnostic](#)
- [Command Line Interface](#)
- [File Editor](#)
- [System Summary](#)
- [VPN Log On](#)
- [IKE/IPSec Configuration](#)

ROUTER INFORMATION	
Product Description	Efficient 5830 DMT Router (5830-006)
Hardware Description	Revision: 002 [S/N:590397]
Software Version	v6.0.150

ROUTER CONFIGURATION	
LAN IP Address	192.168.254.254
WAN Data PVC	not set
WAN Protocol	PPP
WAN Connection Speed	DOWN 0Kb/s : UP 0Kb/s
Bridging	disabled
IP Routing	disabled
WAN IP Address	0.0.0.0
WAN Gateway	
DNS Server Address	0.0.0.0 : 0.0.0.0
Address Translation	disabled

Om door te gaan met de Easy Setup moet u op de Easy Setup-link klikken in het scherm van de Router Information.

Opmerking: U kunt de Easy Setup op ieder gewenst moment van de configuratie afbreken door te klikken op de knop Cancel onder aan het configuratiescherm. Als de procedure wordt geannuleerd, zullen er geen wijzigingen worden aangebracht en de display keert terug naar het scherm Router Information.

WAN Interface-scherm

Het scherm van de WAN Interface is het eerste scherm van de Easy Setup-procedure. Gebruik dit formulier voor uw Wide Area Network (WAN)-instellingen. Twee instellingen zijn vereist; Data-PVC en WAN-protocol.

Scherm 27: WAN Interface-scherm

Efficient NETWORKS

Current User: superuser

WAN Interface (Wide Area Network)

The information on this and subsequent screens is obtained from your service provider.

WAN Protocol

The **Point-to-Point Protocol (PPP)** describes a means to automatically configure a connection for authenticated users.

RFC 1483 describes methods of encapsulating network data traffic over ATM networks.

RFC 1483 MAC Encapsulated Routing (MER) uses the bridged encapsulation method from RFC 1483. This option is selected when the Network Service Provider offers a bridged network but IP routing is desired on the LAN.

[Home](#)

WAN Interface

Data PVC (VPI*VCI) 0 * 35

WAN Protocol

☒ Point-to-Point Protocol over ATM

☐ Point-to-Point Protocol over Ethernet over PPPoA

☐ Point-to-Point Protocol over Ethernet over RFC1483

☐ RFC 1483

☐ RFC 1483 MAC Encapsulated Routing (MER)

☐ RAWIP

Next Cancel

In het scherm WAN Interface kunt u beginnen met de volgende stappen van de Easy Setup.

- Stap 1:** Voer de ATM Permanent Virtual Circuit (PVC)-informatie in. Dit zijn de twee nummers die u van uw netwerkprovider dient te ontvangen.
- Stap 2:** Kies het WAN-protocol dat u wilt gebruiken door te klikken op de betreffende radioknop.
- Stap 3:** Klik op Next om door te gaan met Easy Setup. Het volgende scherm dat verschijnt varieert alnaargelang het protocol dat u hebt gekozen:
- [Point-to-Point Protocol via ATM](#)
 - [Point-to-Point Protocol via Ethernet via ATM](#)
 - [Point-to-Point Protocol via Ethernet via RFC 1483](#)
 - [RFC 1483 Networking](#)
 - [RFC 1483 MAC Encapsulated Routing](#)

Point-to-Point Protocol via ATM

Als u Point-to-Point Protocol over ATM als WAN-protocol hebt geselecteerd, zal Easy Setup het volgende PPP-configuratiescherm weergeven.

Scherf 28: Point-to-Point Protocol via ATM-scherf

Efficient NETWORKS

Current User: superuser

Point-to-Point Protocol (PPP)

PPP usually requires a username and password.

Bridging designates that all traffic to remote hosts that is not routed will be forwarded.

IP Routing routes IP traffic to remote hosts.

The **IP address and Subnet Mask** define the IP address and network of the interface. This information is required in order to use NAT.

The **Default Gateway** is the IP address of the next-hop router.

Network Address Translation (NAT) makes all connections appear to originate from the IP address of this interface.

NetBIOS is a PC networking protocol that may keep connections open inadvertently, thus incurring expenses.

Point-to-Point Protocol (PPP)

PPP username:

PPP password:

PPP Networking

☐ Bridging enabled

☐ Only bridge PPPOE traffic

☐ IP routing enabled

☒ Obtain configuration automatically from WAN

☐ Configure IP Routing manually

Source WAN IP Address

Source Subnet Mask

Default Gateway

☐ NAT enabled

☐ Block NetBIOS traffic

Om door te gaan met PPP via ATM als uw WAN-protocol moet u de volgende stappen uitvoeren:

- Step 1:** Voer de naam van de gebruiker in het veld PPP User Name in en het wachtwoord in het veld Password. Deze informatie krijgt u normaliter van uw netwerkprovider. U hebt een PPP user name en een password nodig voor de aanmelding zodra de netwerkverbinding tot stand is gekomen.
- Step 2:** Klik op de radioknoppen om uit de volgende PPP-networkingopties te kiezen:
- **Bridging Enabled** - Bridging zorgt voor de overdracht van verkeer bestemd voor remote hosts, die niet is gerouted (non-IP) naar het WAN. Als Bridging Enabled is ingesteld, kunt u Only bridge PPPOE traffic selecteren. Door deze optie te kiezen wordt alleen het verkeer via PPPOE ge-bridged. Het overige verkeer wordt afgewezen.
 - **IP Routing Enabled** - IP Routing zal alle IP-pakketten naar het WAN routen die bestemd zijn voor andere hosts. Klik, als de IP Routing Enabled is geactiveerd, om de volgende opties te selecteren:
 - **NAT Enabled** - Network Address Translation (NAT) maakt het mogelijk dat diverse workstations binnen uw LAN één public IP-adres delen. Alle uitgaande verkeer blijkt afkomstig te zijn van het IP-adres van de router.
 - **Block NetBIOS Traffic** - NetBIOS is een netwerkprotocol waarmee netwerkverbindingen onmerkbaar geopend kunnen worden gehouden. Om buitensporige verbindingskosten te vermijden dient dit soort verkeer worden tegengegaan in een netwerkdienst.
- Step 3:** Klik op Next om door te gaan met de configuratie van het Dynamic Host Configuration Protocol in Easy Setup.

Point-to-Point Protocol via Ethernet via PPPoA

Als u Point-to-Point Protocol over Ethernet over PPPoA als WAN-protocol hebt geselecteerd, zal Easy Setup het volgende PPPoE Configuration-scherm weergeven.

Scherm 29: PPPoE configuratiescherm

Efficient NETWORKS

Current User: superuser

Point-to-Point Protocol over Ethernet over PPPoA

PPPoE requires a username and password.

PPPoE Service Name requires a name. Default is * for any.

PPPoE Timer requires a specific duration (in seconds) or the default permanent setting.

PPPoE only Filter is used to specify that only PPPoE traffic will be bridged.

PPPoA Setting is used for PPPoE over PPPoA.

PPPoE Setting

Username:

Password:

Service Name:

PPPoE Timer:

☐ PPPoE only Filter

PPPoA Setting

Username:

Password:

Om door te gaan met PPPoE als uw WAN-protocol moet u de volgende stappen uitvoeren:

- Stap 1:** Voer de naam van de gebruiker in het veld PPP User Name in en het wachtwoord in het veld Password. Deze informatie krijgt u normaliter van uw netwerkprovider. U hebt een PPP user name en een password nodig voor de aanmelding zodra de netwerkverbinding tot stand is gekomen.
- Stap 2:** Voer de PPPoE Service Name in het betreffende veld in. PPPoE vereist de domeinnaam van uw netwerkprovider. Stel * als standaard in (voor alle diensten). Voer de domeinnaam (domain name) in van uw netwerk-serviceprovider in het veld Service Name.
- Stap 3:** Voer de timeout interval (in seconden) in het veld PPPoE Timer in. PPPoE Timer voorziet in een timeout-interval voor perioden waarin geen activiteiten plaatshebben. Na afloop van de opgegeven tijd (in seconden) wordt de PPP-verbinding afgesloten om de kosten van uw verbinding te beperken. De standaardinvoer van
- Stap 4:** Klik hier om een PPPoE only Filter uit te kiezen, als dit nodig mocht blijken. Deze keuze filtert het gehele verkeer 'on the bridge' en zal alleen PPPoE toelaten. Klik op dit vakje als u alleen een verbinding met uw netwerkdienst tot stand wilt brengen via PPPoE.
- Stap 5:** Klik op Next om door te gaan met de configuratie van het Dynamic Host Configuration Protocol in Easy Setup.

Point-to-Point Protocol via Ethernet via RFC 1483

Als u Point-to-Point Protocol over Ethernet over RFC 1483 als WAN-protocol hebt geselecteerd, zal Easy Setup het volgende PPP-configuratiescherm weergeven.

Scherf 30: PPPoE over RFC 1483 configuratiescherm

Current User: superuser

Point-to-Point Protocol over Ethernet over RFC1483

PPPoE requires a username and password.

PPPoE Service Name requires a name. Default is * for any.

PPPoE Timer requires a specific duration (in seconds) or the default permanent setting.

PPPoE only Filter is used to specify that only PPPoE traffic will be bridged.

[Home](#)

PPPoE Setting

Username:

Password:

Service Name

PPPoE Timer

☐ PPPoE only Filter

Previous Next Cancel

Om door te gaan met PPPoE als uw WAN-protocol moet u de volgende stappen uitvoeren:

- Stap 1:** Voer de naam van de gebruiker in het veld PPP User Name in en het wachtwoord in het veld Password. Deze informatie krijgt u normaliter van uw netwerkprovider. U hebt een PPP user name en een password nodig voor de aanmelding zodra de netwerkverbinding tot stand is gekomen.
- Stap 2:** Voer de PPPoE Service Name in het betreffende veld in. PPPoE vereist de domeinnaam van uw netwerkprovider. Stel * als standaard in (voor alle diensten). Voer de domeinnaam (domain name) in van uw netwerk-serviceprovider in het veld Service Name.
- Stap 3:** Voer de timeout interval (in seconden) in het veld PPPoE Timer in. PPPoE Timer voorziet in een timeout-interval voor perioden waarin geen activiteiten plaatshebben. Na afloop van de opgegeven tijd (in seconden) wordt de PPP-verbinding afgesloten om de kosten van uw verbinding te beperken.
- Stap 4:** Klik hier om een PPPoE only Filter uit te kiezen, als dit nodig mocht blijken. Deze keuze filtert het gehele verkeer 'on the bridge' en zal alleen PPPoE toelaten. Klik op dit vakje als u alleen een verbinding met uw netwerkdienst tot stand wilt brengen via PPPoE.
- Stap 5:** Klik op Next om door te gaan met de configuratie van het Dynamic Host Configuration Protocol in Easy Setup.

RFC 1483 Networking

Als u RFC 1483 als WAN-protocol hebt geselecteerd, zal Easy Setup het volgende RFC 1483 Networking-scherm weergeven.

Scherm 31: RFC 1483 Networking-scherm

Efficient NETWORKS

Current User: superuser

RFC 1483 Networking

Bridging designates that all traffic to remote hosts that is not routed will be forwarded.

IP Routing routes IP traffic to remote hosts.

The **IP address and Subnet Mask** define the IP address and network of the interface. This information is required in order to use NAT.

Network Address Translation (NAT) makes all connections appear to originate from the IP address of this interface.

NetBIOS is a PC networking protocol that may keep connections open inadvertently, thus incurring excess charges in fee-for-service agreements.

[Home](#)

RFC 1483 Networking

☐ Bridging enabled

☐ Only bridge PPPOE traffic

☐ IP routing enabled

☒ Obtain configuration automatically from WAN using DHCP

☐ Configure IP Routing manually

IP Address

Subnet Mask

☐ NAT enabled

☐ Block NetBIOS traffic

Om door te gaan met RFC 1483 als uw WAN-protocol moet u de volgende stappen uitvoeren:

Stap 1: Klik hier om een van de volgende mogelijkheden te kiezen:

- **Bridging enabled** - Als Bridging is ingeschakeld, zal alle verkeer voor remote computers dat niet is gerouted, worden doorgestuurd met behulp van bridging.
- **IP routing enabled** - Als IP routing is geselecteerd, voorziet deze optie ook in de velden IP address en subnet mask. Deze kunt u automatisch van uw serviceprovider ontvangen door te klikken op de radioknop met het opschrift 'Obtain configuration automatically from WAN using DHCP'. Als u van uw serviceprovider een specifiek IP-adres en een subnetmasker hebt gekregen, kunt u deze ook handmatig invoeren. Om dit te kunnen doen, moet u op de radioknop namens 'Configure IP Routing manually' klikken en het adres en masker in de betreffende velden invoeren.

Opmerking: Als uw netwerkprovider geen specifieke informatie heeft verstrekt m.b.t. deze instellingen, kies dan IP Routing, Obtain configuration automatically from WAN en NAT enabled.

Stap 2: Als u Bridging enabled hebt gekozen, kunt u optioneel ook Only bridge PPPoE Traffic selecteren. Door deze optie te kiezen wordt alleen het verkeer via PPPoE ge-bridged. Het overige verkeer wordt afgewezen.

Stap 3: Als u IP Routing enabled hebt gekozen, kunt u ook nog de volgende opties selecteren:

- **NAT Enabled** - Network Address Translation (NAT) maakt het mogelijk dat diverse workstations binnen uw LAN één public IP-adres delen. Alle uitgaande verkeer blijkt afkomstig te zijn van het IP-adres van de router.

- Block NetBIOS Traffic - NetBIOS is een netwerkprotocol waarmee netwerkverbindingen onmerkbaar geopend kunnen worden gehouden. Om buitensporige verbindingskosten te vermijden dient dit soort verkeer worden tegengegaan in een netwerkdienst.

Stap 4: Klik op Next om door te gaan met de configuratie van het Dynamic Host Configuration Protocol in Easy Setup.

RFC 1483 MAC Encapsulated Routing

Als u RFC 1483 MAC Encapsulated Routing als WAN-protocol hebt geselecteerd, zal Easy Setup het volgende RFC 1483 MER Networking-scherm weergeven.

Scherm 32: RFC 1483 MAC Encapsulated Routing Network-scherm

Efficient NETWORKS

Current User: superuser

RFC 1483 MER Networking

Bridging designates that all traffic to remote hosts that is not routed will be forwarded.

IP Routing routes IP traffic to remote hosts.

The **IP address and Subnet Mask** define the IP address and network of the interface. This information is required in order to use NAT.

The **Default Gateway** is the IP address of the next-hop router.

Network Address Translation (NAT) makes all connections appear to originate from the IP address of this interface.

NetBIOS is a PC networking protocol that may keep connections open inadvertently, thus incurring excess charges in fee-for-service agreements.

[Home](#)

RFC 1483 MER Networking

☐ Bridging enabled

☐ Only bridge PPPOE traffic

☐ IP routing enabled

☒ Obtain configuration automatically from WAN using DHCP

☐ Configure IP Routing manually

IP Address

Subnet Mask

Default Gateway

☐ NAT enabled

☐ Block NetBIOS traffic

Om door te gaan met RFC 1483 MER als WAN-protocol, moet u de volgende stappen uitvoeren:

Stap 1: Klik hier om een van de volgende mogelijkheden te kiezen:

- Bridging enabled - Als Bridging is ingeschakeld, zal alle verkeer voor remote computers dat niet is gerouted, worden doorgestuurd met behulp van bridging.
- IP routing enabled - Als IP routing is geselecteerd, voorziet deze optie ook in de velden IP address en subnet mask. Deze kunt u automatisch van uw serviceprovider ontvangen door te klikken op de radioknop met het opschrift 'Obtain configuration automatically from WAN using DHCP'. Als u van uw serviceprovider een specifiek IP-adres en een subnetmasker hebt gekregen, kunt u deze ook handmatig invoeren. Om dit te kunnen doen, moet u op de radioknop namens 'Configure IP Routing manually' klikken en het adres en masker in de betreffende velden invoeren.

Opmerking: Als uw netwerkprovider geen specifieke informatie heeft verstrekt m.b.t. deze instellingen, kies dan IP Routing, Obtain configuration automatically from WAN en NAT enabled.

- Stap 2:** Als u Bridging enabled hebt gekozen, kunt u optioneel ook Only bridge PPPoE Traffic selecteren. Door deze optie te kiezen wordt alleen het verkeer via PPPoE ge-bridged. Het overige verkeer wordt afgewezen.
- Stap 3:** Als u IP Routing enabled hebt gekozen, kunt u ook nog de volgende opties selecteren:
- NAT Enabled - Network Address Translation (NAT) maakt het mogelijk dat diverse workstations binnen uw LAN één public IP-adres delen. Alle uitgaande verkeer blijkt afkomstig te zijn van het IP-adres van de router.
 - Block NetBIOS Traffic - NetBIOS is een netwerkprotocol waarmee netwerkverbindingen onmerkbaar geopend kunnen worden gehouden. Om buitensporige verbindingskosten te vermijden dient dit soort verkeer worden tegengegaan in een netwerkdienst.
- Stap 4:** Klik op Next om door te gaan met de configuratie van het Dynamic Host Configuration Protocol in Easy Setup.

Dynamic Host Configuration Protocol

De volgende stap van de Easy Setup is de configuratie van het DHCP. DHCP wijst op dynamische wijze IP-configuratiegegevens toe aan apparaten in het netwerk, waarmee wordt voorkomen dat deze gegevens bij elk apparaat afzonderlijk met de hand moeten worden ingesteld. Dit configuratiescherm voorziet ook in configuratieopties van de DNS (Domain Name Service). DNS zet de namen van hosts om in IP-adressen.

Scherf 33: Dynamic Host Configuration Protocol-scherf

Efficient NETWORKS

Current User: superuser

Dynamic Host Configuration Protocol (DHCP)

DHCP assigns IP configuration information to hosts on the LAN thus avoiding the need for manual setup.

Domain Name Service (DNS) maps names to addresses.

The **Domain Name** identifies the default network name.

Domain Name Servers map host names to IP addresses.

Windows Internet Naming Service (WINS) maps NetBIOS names to IP addresses.

[Home](#)

Dynamic Host Configuration Protocol (DHCP)

☒ DHCP server enabled on LAN

☒ Obtain DNS information automatically
☐ Configure DNS manually

Domain Name

Primary DNS Server

Secondary DNS Server

Primary WINS Server

Secondary WINS Server

Voer de volgende stappen uit om DHCP te configureren:

- Stap 1:** Optioneel kunt u ook hierop klikken om een DHCP-server uit te kiezen die niet actief is binnen het LAN. Als u deze optie selecteert, kan de DHCP-server IP-adresinformatie dynamisch toekennen aan alle apparaten binnen het lokale netwerk.
- Stap 2:** Configureer de Domain Name Service. Kies een van de opties uit:
- DNS-informatie automatisch ontvangen. Door deze optie te kiezen, wordt DNS geactiveerd binnen de router. Het DNS-serveradres wordt bekend zodra verzoeken van de DHCP-client via de WAN-link worden geplaatst.

- Configureer DNS met de hand. Voor de handmatige configuratie van DNS hebt u ten minste één DNS-serveradres nodig en één domeinnaam. Deze informatie krijgt u normaliter van uw netwerkprovider. Voer de DNS-informatie in zoals hierna is beschreven:
1. Voer de domeinnaam in het veld Domain Name in. Hiermee wordt de domeinnaam van de DNS ingesteld.
 2. Voer het IP-adres van de Primary DNS Server in het betreffende veld in. Dit gebeurt indien DNS-aanvragen worden verstuurd.
 3. Optioneel kunt u het IP-adres van de tweede DNS-server in het betreffende veld opgeven. Dit gebeurt indien DNS-aanvragen worden verstuurd terwijl de eerste DNS-server niet beschikbaar is.
 4. Voer het IP-adres van de Primary WINS Server in het betreffende veld in. Net als DNS kent ook de Windows Internet Naming Service (WINS) namen van NetBIOS toe aan IP-adressen. Dit gebeurt indien WINS-aanvragen worden verstuurd.
 5. Optioneel kunt u het IP-adres van de tweede WINS-server in het betreffende veld opgeven. Dit gebeurt indien WINS-aanvragen worden verstuurd terwijl de eerste WINS-server niet beschikbaar is.

Stap 3: Klik op Next om door te gaan met Easy Setup.

Configuratie van een Local Area Network

Het laatste scherm van de Easy Setup is dat van de Local Area Network (LAN)-configuratie.

Scherf 34: Local Area Network-configuratiescherf

Efficient NETWORKS®

Current User: superuser

LAN IP Configuration

The **IP Address** is the network address of the router. This address must be globally unique unless NAT is enabled.

Subnet Mask is used along with the IP address to determine whether or not the local IP traffic should be forwarded.

[Home](#)

LAN IP Configuration	
IP Address	192.168.254.254
Subnet Mask	255.255.255.0

Previous Save and Reboot Cancel

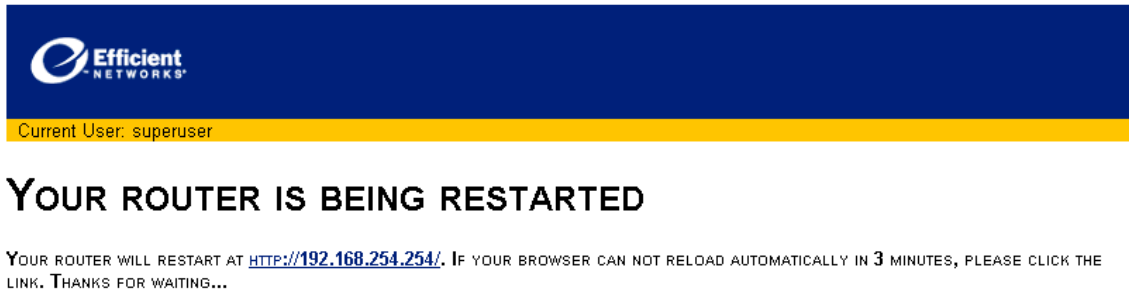
Om door te gaan met de configuratie van uw Local Area Network, moet u de volgende stappen uitvoeren:

- Stap 1:** Voer het IP-adres in het veld IP address in. Het IP-adres is het netwerk adres van uw router. Dit adres moet uniek zijn tenzij NAT ingeschakeld is.
- Stap 2:** Voer het subnetmasker in het veld Subnet Mask in. Het subnetmasker wordt samen met het IP-adres gebruikt om vast te stellen of IP-verkeer binnen het LAN naar het WAN moet worden doorgestuurd.
- Stap 3:** Klik op de knoppen Save en Reboot.

Wijzigingen die tijdens de Easy Setup-procedure zijn aangebracht, worden opgeslagen en permanent met behulp van rebootfuncties van het systeem. De router wordt opnieuw gestart met de nieuwe configuratie-instellingen.

Restarting Router-scherm

Scherm 35: Restarting Router-scherm



U moet een login uitvoeren om de rebootprocedure af te sluiten. Als het scherm van de Router Information niet binnen drie minuten verschijnt, klik op de link in de herstartmelding om uw netwerkverbinding opnieuw tot stand te brengen. De melding is hieronder te zien.

Uw router zal een herstart uitvoeren bij <http://192.168.254.254>. Als uw browser niet binnen drie minuten een automatische reload maakt, klik dan op de link. Bedankt voor uw geduld...

GEAVANCEERDE FACILITEITEN

U hebt de beschikking over geavanceerde faciliteiten die zowel gewone systeemoperaties als geavanceerde routerfuncties omvatten. Kies uit de onderstaande lijst als u meer wilt weten over het configureren van (een van) deze faciliteiten.

- [Access Control](#) - Met behulp van de faciliteit Access Control kan de toegang en controle van uw router worden beperkt tot een bepaalde groep van hosts. Access Control wordt gebruikt om de toegang tot uw systeem te configureren.
- [User Management](#) - Deze faciliteit voorziet in het management van User Accounts. Deze User Accounts voorzien in de toegang tot het besturingssysteem en de commando's van de router. Deze faciliteit ondersteunt een role-based management van max. 15 gebruikers. Elke gebruiker kan over specifieke toegangs- en managementrechten beschikken. Het aantal User Accounts kan worden verhoogd met behulp van de optionele faciliteit RADIUS.
- [Router Clock](#) - In dit scherm kan de router clock worden ingesteld en gewijzigd, inclusief de mogelijkheid van synchronisatie met een werkstation.
- [DHCP](#) - De faciliteit DHCP Configuration stelt u in staat om de bestaande Dynamic Host Configuration Protocol (DHCP)-instellingen van uw router te bekijken en nieuwe te maken. DHCP is een TCP/IP-serviceprotocol dat voorziet in de dynamische toekenning van IP-adressen en andere configuratie-informatie aan client hosts binnen een netwerk.
- [NAT](#) - Network Address Translation wordt gebruikt voor het vertalen van adressering tussen een LAN en WAN. Network Address Translation (NAT) is een faciliteit die voorziet in een bepaald veiligheidsniveau door het eigen IP-adres van uw LAN achter het enige public IP-adres van uw router te verstoppen. Network Address Translation kan voorzien in een stukje veiligheid met behulp van onduidelijkheid waarmee de meeste gebruikers wel kunnen leven.
- [SNMP](#) - SNMP maakt het management mogelijk van netwerkknooppunten via de uitwisseling van meldingen tussen een management client en een management agent. Deze meldingen kunnen worden gebruikt om de systeemstatus uit op te maken of om operationele parameters in te stellen waar dit wordt ondersteund.
- [Secure Shell \(SSH\)](#) - Secure Shell (SSH) stelt de ontvangst zeker van veilige netwerkdiensten via onveilige netwerken, zoals internet.
- [Firewall Scripts](#) - Met deze scripts kunnen snel en gemakkelijk robuuste IP filterende firewalls worden gemaakt. De scripts kunnen ook worden gewijzigd om tegemoet te komen aan individuele vereisten.
- [Quality of Service \(QoS\)](#) - Quality of Service (QoS) is een reeks faciliteiten die wordt gebruikt voor een actief management van de bandbreedte van een netwerk om serviceniveaus voor prioritaire toepassingen te ondersteunen.
- [Stateful Firewall](#) - De router beschikt over twee typen van een firewall: de ene is een IP filterende firewall, de andere een Stateful Firewall, die voorziet in een robuustere, sessiegebaseerde netwerkbeveiliging. Stateful firewalls registreren de context van de verbindingen gedurende elke sessie door een voortdurende update van de toestandsgegevens in dynamische tabellen. Stateful firewalls maken een intellegentere, meer flexibele en robuuste benadering van netwerkbeveiliging mogelijk met betere afwerpmethoden dan de stateless IP filterende firewalls.
- [Dial Backup](#) - Dial Backup voorziet in een backup-verbinding met uw serviceprovider via een modem. Deze backup-link kan geactiveerd worden in het geval van een storing of onderbreking van uw eerste WAN-dienst.
- [Diagnostic](#) - De faciliteit Diagnostic van uw router wordt gebruikt voor het opsporen van technische problemen en om de status van uw routerfuncties te testen.
- [File Editor](#) - De faciliteit File Editor voorziet in de mogelijkheid om bestanden te maken of te wijzigen, die op uw router zijn opgeslagen.
- [Command Line Interface](#) - De faciliteit Command Line Interface voorziet in een toegangspunt tot de Command Line Interface van de webinterface. De commando's kunnen direct in dit scherm worden ingevoerd, terwijl de outputs eveneens meteen in hetzelfde venster worden weergegeven.
- [IKE/IPSec Configuration](#) - Internet Key Exchange/Internet Protocol Security (IKE/IPSec) is een veiligheidsfunctie voor de authenticatie en encryptie van IP-verkeer voor de authenticiteit, integriteit en privacy van uw verbindingen.

Access Control

Het scherm Access Control wordt gebruikt om toegangsrestricties tot het systeem in te stellen. Elke remote access-methode kan worden gezet op een van de drie mogelijke toegangsniveaus; zie hierna.

Scherf 36: Access Control-scherf

Efficient NETWORKS

Current User: superuser

Access Control

Access Control restricts administrative control of the router to a specific set of IP addresses.

No access restrictions allows access from all hosts.

Allowed from LAN limits access to hosts on the LAN.

[Home](#)

Access Control

- ☒ Enable Telnet Management
 - ☒ No access restrictions
 - ☐ Allowed from LAN
- ☒ Enable Web Management
 - ☒ No access restrictions
 - ☐ Allowed from LAN
- ☒ Enable SNMP Management
 - ☒ No access restrictions
 - ☐ Allowed from LAN
- ☒ Allow System Logging to Syslog Servers
 - ☒ No access restrictions
 - ☐ Restricted to servers on LAN

Save and Reboot

De drie niveaus van toegangscontrole van elke toegangsmethode zijn:

- Geactiveerd zonder toegangsbeperking. Om een toegangsniveau in te stellen voor een bepaalde methode, moet het controlevakje zijn aangekruist voor u op de knop No access restrictions klikt.
- Geactiveerd, maar alleen met toegang via het LAN. Om een toegangsniveau in te stellen voor een bepaalde methode, moet het controlevakje zijn aangekruist voor u op de knop Allowed from LAN klikt.
- Gedeactiveerd en toegang niet geoorloofd. Om een toegangsmethode ongedaan te deactiveren, moet u zich ervan vergewissen dat het controlevakje leeg is en er geen andere knoppen zijn geselecteerd.

Klik op de knoppen Save en Reboot zodat uw wijzigingen van kracht worden.

Opmerking: Als u niet precies weet hoe u de Access Control moet configureren, laat dan gewoon de fabrieksmatige standaardinstellingen staan. U kunt deze instellingen op ieder gewenst moment wijzigen door terug te keren naar het scherm Access Control.

User Management

De faciliteit User Management voorziet in het management van User Accounts. Deze User Accounts voorzien in de toegang tot het besturingssysteem en de commando's van de router.

User Management-scherm

Het scherm User Management toont een lijst van de huidige User Accounts en functies voor deze User Accounts. De functies van het User Management zijn:

- [Maak een nieuw User Account](#)
- [Hoe wijzigt u een User Account?](#)
- [Hoe verwijdt u een User Account?](#)

Daarnaast voorziet het scherm in de toegang tot geavanceerde functies:

- [User Lookup Configuration](#)
- [Secure Mode Configuration](#)

Het scherm User Management is hieronder te zien:

Scherm 37: User Management-scherm

The screenshot shows the User Management interface. At the top, there is a blue header with the Efficient Networks logo. Below the header, a yellow bar indicates the current user is 'superuser'. The main content area is divided into two sections. On the left, a grey sidebar contains the title 'User Management', a description of its functions, and links for 'User Lookup Config', 'Secure Mode Config', and 'Home'. On the right, a white box titled 'Select User' contains a dropdown menu with 'superuser' selected. Below this box are three buttons: 'New User', 'Edit User', and 'Delete User'.

Een nieuwe User Account toevoegen

Voer de volgende procedure uit om een nieuwe User Account toe te voegen:

- Step 1:** Klik op New User in het scherm User Management.
Het scherm Add/Modify User verschijnt.

Scherf 38: Add/Modify User-scherf

Efficient NETWORKS

Current User: superuser

Add/Modify User

Used to set the user's access privileges. This includes username, password, management class access, path control access. This page also allows a user to be disabled without removing the user from the database. You must have Admin access to perform these functions. The buttons across the top of the form set the controls below to preset values.

When editing an existing user, the username itself may not be changed. In addition, the password is not displayed. If the administrator leaves the password fields blank, the passwords will not be changed; if the password fields are filled in, the user's password will be changed.

NOTE: The Account Access checkbox for enabling and disabling an account is not automatically checked for a new account. The Administrator MUST check this box in order for the new account to be accessible to a user.

[User Management Main Page](#)
[Home](#)

Add/Modify User

SuperUser NetworkMgr SecurityMgr Viewer

User Name:

Password:

Confirm Password:

Network Access: ☒ None ☐ Read ☐ Read-Write

System Access: ☒ None ☐ Read ☐ Read-Write

Security Access: ☒ None ☐ Read ☐ Read-Write

Admin Access: ☒ None ☐ Read ☐ Read-Write

Debug Access: ☒ None ☐ Read-Write

Allow Access from: ☒ LAN ☒ WAN ☒ Console

Account access: ☐ Enabled

Apply

- Step 2:** Voer de naam van de gebruiker in het veld User Name in.

- Step 3:** Voer het gebruikers-wachtwoord in:

- Voer het wachtwoord in het veld Password in.
- Voer hetzelfde wachtwoord opnieuw in het veld Confirm Password in.

- Step 4:** Specificeer de rechten van de class in het User Account Management. U moet voor elke Activity Class Read / Read-Write-rechten selecteren voor de gebruiker of op None klikken als de gebruiker deze rechten niet mag krijgen.

Opmerking: Bijzondere rechten kunnen met de hand worden ingesteld of met behulp van een User Template, als beschreven in het vorige gedeelte.

- Step 5:** Klik hier om de interface(s) te kiezen via welke de User Account kan worden bereikt: LAN, WAN of Console.

- Step 6:** De User Account staat standaard op disabled. Om toegang tot de User Account te krijgen, moet u op Enable klikken.

- Step 7:** Klik op Apply om een nieuw User Account toe te voegen.

Uw nieuwe User Account is nu beschikbaar.

User Templates

User Templates zijn voorgeconfigureerd ten behoeve van het maken en beheer van User Accounts. Deze sjablonen bevatten voorgedefinieerde rechten, gebaseerd op typische rollen binnen het routerbeheer. Ook al werd er reeds een sjabloon gekozen voor een gebruiker, kunnen de bijzondere rechten van de gebruiker nog steeds met de hand worden gewijzigd. De knoppen boven aan het venster Add/Modify User verschaffen toegang tot de User Templates. Om een User Template op een User Account toe te passen moet u alleen maar op de knop klikken van de gewenste class voor deze User Account. Zodra er een sjabloon is geselecteerd, worden de instellingen van deze sjabloonklasse toegepast op de User Template. U kunt deze instellingen met de hand aanpassen.

Hoe wijzigt u een User Account?

Om een bestaande User Account te wijzigen, moet u de volgende procedure uitvoeren:

- Stap 1:** Klik in het scherm User Management om een User Account te kiezen die u via het menu Select User wilt wijzigen.
- Stap 2:** Klik op de knop Edit User om het scherm Add/Modify User weer te geven. U kunt bij elke gewenste User Account wijzigingen aanbrengen, met uitzondering van de naam van een bestaande User Account, die u niet mag wijzigen.
- Stap 3:** Wijzig het User Password:
 - a. Voer het wachtwoord in het veld Password in.
 - b. Voer hetzelfde wachtwoord opnieuw in het veld Confirm Password in.
- Stap 4:** Specificeer de rechten van de class in het User Account Management. U moet voor elke Activity Class Read / Read-Write-rechten selecteren voor de gebruiker of op None klikken als de gebruiker deze rechten niet mag krijgen.

Opmerking: Bijzondere rechten kunnen met de hand worden ingesteld of met behulp van een User Template als beschreven in het vorige gedeelte.

- Stap 5:** Klik hier om de interface(s) te kiezen via welke de User Account kan worden bereikt: LAN, WAN of Console.
- Stap 6:** Klik om de Account access als enabled in of uit te schakelen. De User Account is pas beschikbaar als u op het controlevakje hebt geklikt.
- Stap 7:** Klik op Apply om de User Account te updaten.



PAS OP! Het wijzigen van het password of bijzonder rechten van een bestaande user account, kan ertoe leiden dat de lopende activiteit van een gebruiker wordt beëindigd.

Hoe verwijdert u een User Account?

Voer de volgende procedure uit om een User Account te verwijderen:

- Stap 1:** Klik in het scherm User Management op de betreffende User Account die u uit het menu Select User wilt verwijderen.
- Stap 2:** Klik op Delete User
- Stap 3:** Klik op OK om het verwijderen van de Account te bevestigen, als hierom wordt gevraagd.

User Lookup Configuration

Het scherm User Lookup Configuration stelt de beheerder in staat om de zoekvolgorde te definiëren (primary en secondary) voor logins van gebruikers. Het scherm User Lookup Configuration is hieronder te zien.

Schermbild 39: User Lookup Configuration-schermbild

Efficient NETWORKS

Current User: superuser

User Lookup Configuration

Allows the user to choose which database is the primary lookup for a user login request. Either the primary or secondary lookup must be Local.

[User Management Main Page](#)

[Home](#)

User Lookup Configuration

Primary: ☒ Local ☐ Radius ☐ None

Secondary: ☐ Local ☐ Radius ☒ None

Apply

De keuzeopties zijn:

- Local - Local zoekt in de database van de lokale gebruikers, die zich in de flash memory bevindt.
- Radius - Radius heeft tot gevolg dat de RADIUS-client een gecodeerd toegangsverzoek tot een geconfigureerde RADIUS-server.
- None - None geeft aan dat alleen de specifieke alternatieve methode gebruikt zal worden voor de zoekacties.

Opmerking: Ten minste één zoekbereik (primary of secondary) zal altijd Local zijn. Door hetzij de eerste, hetzij de tweede voor Radius of None in te stellen, wordt de standaard voor de gewijzigde zoekactie op Local gezet.

Voer de volgende procedure uit om User Lookup te configureren:

- Stap 1:** Klik hier om de Primary zoeklocatie te kiezen.
- Stap 2:** Klik hier om de Secondary zoeklocatie te kiezen.
- Stap 3:** Klik op Apply om de wijzigingen op te slaan.

Secure Mode Configuration

Secure Mode is een faciliteit waarmee de toegang tot het systeem kan worden beperkt tot kanalen die veilig en zeker werken. De Secure Mode kan zowel in verbinding met de WAN interface worden gebruikt als met een, LAN interface of zelfs met beide. Als Secure Mode is geactiveerd, kan een interface in betrouwbaar worden herbenoemd, wat impliceert dat onveilige verbindingen via de betrouwbare interface toegelaten zijn. Het omdopen van een interface in onbetrouwbaar heeft tot gevolg dat een veilig kanaal vereist is voor de toegang via deze onbetrouwbare interface. Standaard staat de WAN-interface op untrusted en de LAN-interface op trusted.

Het Secure Mode Configuration-schermb is hieronder te zien.

Schermb 40: Secure Mode Configuration-schermb

Efficient NETWORKS

Current User: superuser

Secure Mode Configuration

Allows the user to enable or disable secure mode. When Secure Mode is enabled, the WAN and LAN interfaces may be set as trusted or untrusted.

A untrusted interface must come over an encrypted tunnel (such as SSH, or telnet-over-IPSec). A trusted interface may or may not come over an encrypted tunnel.

[User Management Main Page](#)

[Home](#)

Secure Mode Configuration

Secure Mode: ☒ Enabled

LAN Interface: ☒ Trusted ☐ Untrusted

WAN Interface: ☐ Trusted ☒ Untrusted

Apply

Opmerking: Als de Secure Mode is geactiveerd zullen alle bestaande onveilige verbindingen via een onbetrouwbare interface onmiddellijk worden verbroken, behalve die van de ingaande bestandstransfers. Ingaande bestandstransfers worden afgemaakt voor de sessie wordt afgesloten.

Voer de volgende procedure uit om de Secure Mode te configureren:

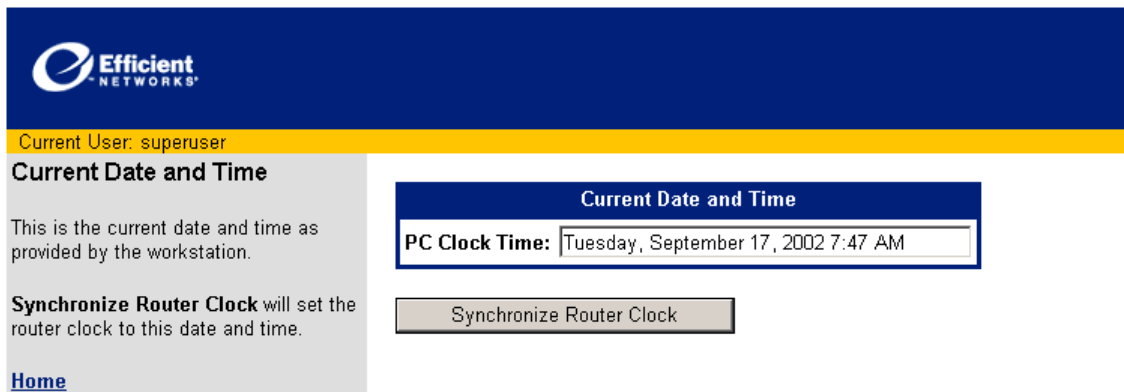
- Stap 1:** Klik op het controlevakje Enabled om de Secure Mode in te schakelen. Als dit vakje leeg is, is de Secure Mode gedeactiveerd.
- Stap 2:** Klik op de knop Trusted of de knop Untrusted om de beveiligingsmodus van de LAN Interface in te stellen.
- Stap 3:** Klik op de knop Trusted of de knop Untrusted om de beveiligingsmodus van de WAN Interface in te stellen.
- Stap 4:** Klik op Apply om de instellingen op te slaan.

Current Date and Time

Met behulp van deze faciliteit kunt u de datum en tijd instellen die uw router registreert. Het veld Current Date and Time toont de huidige datum en tijd van uw pc.

Om de datum en tijd van uw router te synchroniseren met de huidige datum en tijd, moet u op de knop Synchronize Router Clock klikken.

Scherf 41: Current Date and Time-scherf



The screenshot displays the 'Current Date and Time' configuration page of an Efficient Networks router. The page has a dark blue header with the 'Efficient NETWORKS' logo. Below the header, a yellow bar indicates the 'Current User: superuser'. The main content area is divided into two sections. On the left, a grey sidebar contains the title 'Current Date and Time', a description 'This is the current date and time as provided by the workstation.', a note 'Synchronize Router Clock will set the router clock to this date and time.', and a 'Home' link. On the right, a white box with a blue header 'Current Date and Time' contains a text input field labeled 'PC Clock Time:' with the value 'Tuesday, September 17, 2002 7:47 AM'. Below this input field is a button labeled 'Synchronize Router Clock'.

DHCP Configuration

De faciliteit DHCP Configuration stelt u in staat om de huidige Dynamic Host Configuration Protocol (DHCP)-instellingen van uw router te maken en te bekijken. DHCP is een TCP/IP-serviceprotocol dat voorziet in de dynamische toekenning van IP-adressen en andere configuratie-informatie aan client hosts binnen een netwerk. Uw router kan een DHCP-server nabootsen, met een centraal management van uw pool van IP-adressen voor een eenvoudige en veilige TCP/IP-configuratie en toekenning van het IP-adres. Als het DHCP wordt gecombineerd met NAT (Network Address Translation), voegt uw router een veiligheidsmaatregel toe aan uw netwerk door het toekennen en verstoppert van private IP-adressen achter unieke public IP-adressen. Deze privé-IP-adressen voorkomen het ontstaan van extra kosten voor aanvullende public-IP-adressen om een groeiend netwerk te ondersteunen.

Het scherm DHCP Configuration toont de bedienopties die u nodig hebt om het DHCP te configureren; zie hierna.

Scherf 42: DHCP Configuration-scherf

Efficient NETWORKS

Current User: superuser

DHCP Configuration

Trusted Interface DHCP Server Status
Shows the current trusted interface DHCP setting and allows the administrator to enable/disable it.

Trusted Interface DHCP Server Status	
Current Setting	New Setting
Enabled	Enable <input type="button" value="Apply"/>

IP Addresses Pool Setting
Shows the current first IP address and the last IP address in the range of the IP address pool, and enables the administrator to specify a new range of IP addresses. Remember: The last IP address must be greater or equal to the first IP address. Both the first IP address and the last IP address cannot be a subnet address or a broadcast address.

IP Addresses Pool Setting		
	Current Setting	New Setting
First IP Address	192.168.254.2	<input type="text"/>
Last IP Address	192.168.254.20	<input type="text"/>

Current DHCP Leases List

Client IP	State	Host Name	Expires (mm/dd/yy)
192.168.254.2	enabled	icalder	Apr 1 2003 17:07:59

DHCP Configuration bestaat uit de volgende instellingen:

- LAN DHCP Server Status - Deze geeft de huidige DHCP-servermodus aan.
- IP Addresses Pool Setting - Met het DHCP komen alle IP-adressen die toegekend worden aan netwerk-clients, uit een pool. Het **IP Addresses Pool Setting**-gedeelte voorziet in velden om bereiken van IP-adressen mee te definiëren voor uw pool. De velden onder **Current Setting** tonen de actuele IP-adressen in de pool.
- Current DHCP Leases List - Op deze lijst staan de clients die hun IP-adres op dit moment uit de pool halen. De volgende informatie staat van links naar rechts in elke regel:
 - Client IP: Hier staat het tijdelijke IP-adres dat aan de specifieke client is toegekend.
 - State: Geeft aan of het IP-adres geactiveerd of gedeactiveerd is.
 - Host Name: Hier staat de naam van de host die het specifieke IP-adres in gebruik heeft.
 - Vervaldatum (mm/dd/yy): Hier staat de datum waarop het gebruik van het IP-adres zal verstrijken. Op dit moment (en misschien zelfs al eerder) zal het laagste IP-adres worden vrijgegeven om opnieuw

toegekend te kunnen worden zodat de network client de router om de toekenning van een nieuw IP-adres moet vragen.

Om uw DHCP te configureren, moet u de volgende stappen uitvoeren:

Stap 1: Wijzig de huidige DHCP Server Status als gewenst.

- a. Kies de gewenste LAN DHCP Server Status Mode uit het meerkeuzemenu van de New Setting.
- b. Klik op Apply om uw nieuwe LAN DHCP-modus in te stellen.

Stap 2: Definieer het bereik van de IP Address Pool Setting als gewenst.

- a. Voer het eerste IP-adres in het veld First IP Address in.
- b. Voer het laatste IP-adres in het veld Last IP- Address in.
- c. Klik op Apply om uw nieuwe IP-adresbereik in te stellen.

Opmerking: Het laatste IP-adres moet ten minste 1 increment groter zijn dan het eerste IP-adres. Het eerste IP-adres en het laatste IP-adres kunnen geen subnetadres en evenmin een broadcastadres zijn.

Network Address Translation

Network Address Translation (NAT) is een faciliteit die voorziet in een bepaald veiligheidsniveau door het eigen IP-adres van uw LAN achter het enige public IP-adres van uw router te verstoppen. Alle verbindingen moeten via uw router lopen en worden vertaald via NAT. Uw router vertaalt netwerkadressen van inkomend verkeer van public in private IP-adressen en vertaalt adressen van uitgaand verkeer van private IP-adressen in een public IP-adres. Deze translation verstopt de private IP-adressen die binnen het Local Area Network (LAN) worden gebruikt. Network Address Translation kan voorzien in een stukje veiligheid met behulp van onduidelijkheid waarmee de meeste gebruikers wel kunnen leven.

Het scherm NAT Settings voorziet in bedienopties voor het configureren van NAT in uw router.

Scherf 43: NAT Settings-scherf

Efficient NETWORKS

Current User: superuser

NAT Settings

Outbound NAT Setting
Shows current outbound (from LAN to WAN) NAT setting and allows user to enable/disable it.

NAT Passthrough Setting
Provides support for NAT passthrough of multiple VPN PC clients.

Inbound NAT Setting
Provides two ways to configure inbound(WAN to LAN) NAT setting.

- Easy Setup:** User just picks one of the predefined services and provides the IP address of the local machine.
- Advanced Setup:** User can pick a protocol and a pair of ports(first port and last port) from

NAT Settings

Outbound NAT Setting:

WAN <----- Router <----- Local Machine

Current Setting	New Setting	Apply
Disabled	Enable	

NAT Passthrough Setting:

NAT Passthrough

Current Setting	New Setting	Apply
Disabled	Enable	

Inbound NAT Setting:

	WAN ----->	Router	-----> Local Machine
Easy Setup	Service: TELNET		Default Port#: Add
Advanced Setup	Protocol: TCP	First Port#: Last Port#:	IP Address: Port#: Add

Current Inbound NAT Setting:

Protocol	First Port#	Last Port#	IP Address	Port#

Reboot

Outbound NAT Setting

Het veld Outbound NAT Setting wordt gebruikt om Network Address Translation van het uitgaande verkeer in (enable) of uit te schakelen (disable); communicatie van uw LAN naar het Wide Area Network (WAN) buiten de router om. Om de Outbound NAT in te stellen, moet u volgende stappen uitvoeren:

- Stap 1:** Kies Enable uit de meerkeuzelijst onder New Setting om uitgaande NAT te activeren of Disable om uitgaande NAT uit te schakelen.
- Stap 2:** Klik op de knop Apply om uw nieuwe instelling op te slaan.

NAT Passthrough Setting

Het veld NAT Passthrough Setting wordt gebruikt om de NAT Passthrough mode in (enable) of uit te schakelen (disable). Als NAT Passthrough is ingeschakeld (enabled), zijn er multiple Virtual Private Network (VPN)-clients toegestaan. Als NAT Passthrough is gedeactiveerd (disabled), is er slechts één VPN-client toegestaan. Om de modus NAT Passthrough in te schakelen, moet u de volgende stappen uitvoeren:

- Stap 1:** Kies Enable in de meerkeuzelijst onder New Setting om de NAT Passthrough modus te activeren of Disable om deze modus uit te schakelen.
- Stap 2:** Klik op de knop Apply om uw nieuwe instelling op te slaan.

Inbound NAT Setting

Het deel Inbound NAT Setting van het NAT Settings-scherm is verticaal in twee delen opgesplitst:

- Het linkerdeel omvat de velden voor het maken van Wide Area Network (WAN)-instellingen.
- Het rechterdeel omvat velden voor het maken van lokale instellingen.

Een gelabeld gedeelte

Er bestaan twee methoden om ingaande NAT-instellingen te maken:

- [Easy Setup](#)
- [Advanced Setup](#)

Easy Setup

U kunt uw inkomende NAT snel en gemakkelijk configureren met de Easy Setup opdat de meeste gangbare netwerkdiensten worden ondersteund. Om Inbound NAT met behulp van de velden van Easy Setup te configureren, moet u de volgende stappen uitvoeren:

- Stap 1:** Gebruik het meerkeuzemenu Service in het gedeelte WAN ----> om een netwerkdienst te kiezen.
- Stap 2:** Voer in het betreffende veld in het gedeelte ----> Local Machine het IP-adres in van de lokale pc.
- Stap 3:** Kies een van de volgende opties in het gedeelte ----> Local Machine:
- Stel de Default Port# in van de betreffende netwerkdienst door te klikken op de aangrenzende Add-knop.
 - Voeg een nieuw poortnummer toe door het gewenste nummer op te geven in het veld Port# en bevestig deze invoer door te klikken op de aangrenzende knop Add.

Advanced Setup

De velden van de Advanced Setup voorzien in de optie om bepaalde netwerkprotocollen toe te kennen aan bepaalde poorten aan de WAN-zijde van NAT, terwijl de WAN-instellingen worden gemapd aan de IP-adressen en poortnummers van een lokale pc. Advanced Setup kan worden aangevuld met de volgende operaties:

- Stap 1:** Gebruik het meerkeuzemenu Protocol in het gedeelte WAN ----> om een netwerkprotocol te kiezen.
- Stap 2:** Voer de eerste poort in het veld First Port# en de laatste poort in het veld Last Port# in om een reeks van poorten toe te kennen aan het netwerkprotocol dat u hebt gekozen.
- Stap 3:** Kies een van de volgende opties in het gedeelte ----> Local Machine:
- Stel de Default Port# in van het betreffende netwerkprotocol door te klikken op de aangrenzende Add-knop.
 - Voeg een nieuw poortnummer toe door het gewenste nummer op te geven in het veld Port# en bevestig deze invoer door te klikken op de aangrenzende knop Add.
- Stap 4:** Herhaal deze procedure voor elk protocol dat u voor NAT wilt configureren.

Klik op de knop Reboot om uw router met de nieuwe NAT-instellingen te herstarten .

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) voorziet in de uitwisseling van meldingen tussen een netwerkmanagement client en een netwerkmanagement agent voor remote management of netwerkknooppunten. Deze meldingen bevatten aanvragen voor het ontvangen en instellen van variabelen van netwerkknooppunten ten behoeve van het maken van statistieken, instellen van configuratieparameters en om netwerkevents te volgen. SNMP-communicatie is mogelijk via een LAN- of WAN-verbinding.

SNMP Configuration-scherm

Scherf 44: SNMP Configuration-scherm

The screenshot displays the 'SNMP Configuration' window. On the left, there is a sidebar with the 'Efficient NETWORKS' logo, the current user 'superuser', and links for 'SNMP IP Filter', 'SNMP Password', and 'Home'. The main configuration area includes the following fields and options:

- Community String:** A text input field containing 'public'.
- Write Community String:** A text input field containing 'public'.
- Port Number:** A text input field containing '161', with radio buttons for 'Port Number' (selected), 'Disable', and 'Default'.
- Enabled Interfaces:** Two checked checkboxes for 'LAN' and 'WAN'.
- Trap Enable:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Trap Manager 1, 2, 3, 4:** Four empty text input fields for specifying trap manager IP addresses.

Met behulp van het SNMP-configuratiescherm kunnen de bestaande SNMP-instellingen worden bekeken en geconfigureerd. Bij deze instellingen horen:

- **Community String** - Dit veld identificeert de SNMP-community waartoe de router behoort. De community gedraagt zich als een identifier van de meldingen tussen de SNMP-manager en de agent. De instellingen voor de community stellen de SNMP-manager in staat informatie van een hele community op te vragen in plaats van elk afzonderlijk knooppunt (agent).
- **Port Number** - In dit veld wordt de SNMP-poort ingesteld. De SNMP-poort kan worden uitgeschakeld (disabled), op de standaardwaarde van 161 worden gezet of opnieuw worden gedefinieerd en van een non-standaard waarde voorzien die u zelf bepaalt.
- **Enabled Interfaces** - Deze controlevakjes bepalen of de interfaces beschikbaar zijn voor SNMP.
- **Trap Enable** - Met deze instelling kan de SNMP-trap worden in- (enable) of uitgeschakeld (disable). SNMP-agenten hebben de mogelijkheid om ongevraagd meldingen te versturen aan de SNMP-managers. De meldingen worden ook wel 'traps' genoemd en maken de SNMP-managers attent op events binnen het netwerk.
- **Trap Manager** - Deze velden, genummerd van 1 tot 4, worden gebruikt om de IP-adressen te specificeren voor SNMP-managers die een trap event van de router ontvangen.

Voer de volgende procedure uit om SNMP te configureren:

Stap 1: Voer de Community String in het betreffende veld in.

- Stap 2:** Benoem het SNMP Port Number in door middel van een van de volgende opties:
- Default - Klik op deze knop om de SNMP-poort op de standaard van 161 te zetten en SNMP mogelijk te maken.
 - Disable - Klik op deze knop om de SNMP-poort te deactiveren door deze op 0 (nul) te zetten.
 - Port Number - Klik op deze knop om een non-standaard poort te definiëren voor het SNMP. Voer het gewenste poortnummer in het betreffende veld in. U mag een getal kiezen tussen 1 en 65535.
- Stap 3:** Klik hier om de Enabled Interfaces te kiezen die u wilt gaan gebruiken met SNMP.
- Stap 4:** Klik hier om Trap Enable op Enable of Disable te zetten.
- Stap 5:** Voer het IP-adres in van alle Trap Managers (1-4) in de betreffende velden. De velden mogen leeg blijven als u de traps hebt uitgeschakeld.
- Stap 6:** Klik op de knop Apply om uw SNMP-configuratie op te slaan en te activeren.

SNMP IP Filter

Het SNMP IP Filter-configuratiescherm voorziet in instellingen voor IP-adresbereiken om de SNMP-meldingen te filteren. Door een SNMP IP filter in te stellen worden de SNMP-meldingen beperkt tot dewelke die afkomstig zijn van het opgegeven IP-adresbereik. Het LAN kan worden vrijgesteld van IP-filtering. Alle huidige SNMP IP-adresfilters staan in het schermdeel met de IP-adressen.

Scherf 45: SNMP IP Filter Configuration-scherf

Efficient NETWORKS

Current User: superuser

SNMP IP Filter Configuration

Activating an IP Filter range will limit SNMP requests to ONLY those that originate from these addresses.

[SNMP Main Page](#)

[Home](#)

IP Addresses	
Beginning IP Addr.	Ending IP Addr.

Add an IP Range

To Add a IP Range, enter the IP Range or check LAN:

Start IP Range:

End IP Range:

LAN: ☐

Add IP Range

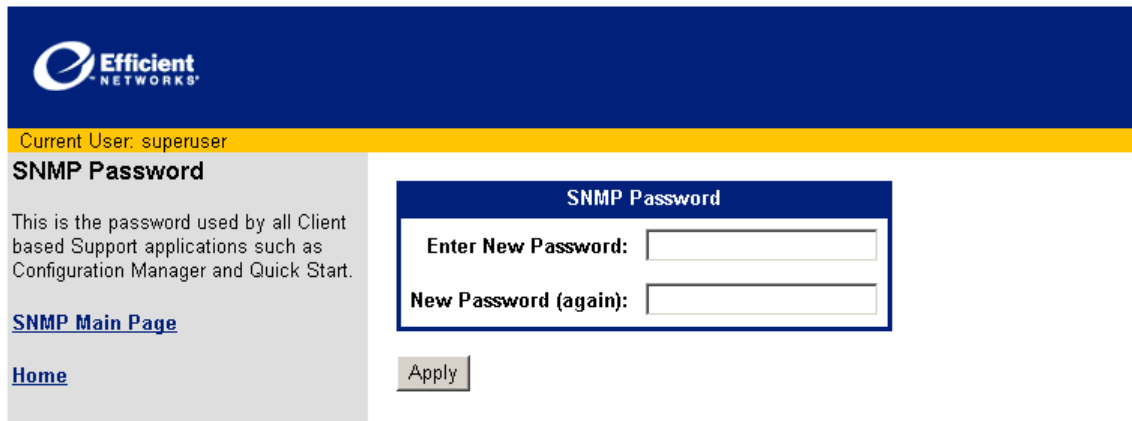
U kunt een nieuwe SNMP IP-filter toevoegen met behulp van de volgende procedure:

- Stap 1:** Voer het eerste IP-adres in het filterbereik in het veld Start IP Range in het gedeelte Add an IP Range.
- Stap 2:** Voer het laatste IP-adres in van het filterbereik in het veld End IP Range.
- Stap 3:** Klik op het controlevakje LAN om in te stellen dat de LAN-interface niet onderhevig zal zijn aan SNMP IP-filtering.
- Stap 4:** Klik op de knop Add IP Range om uw nieuwe SNMP IP Filter te activeren. Het scherm wordt geactualiseerd en het nieuwe SNMP IP-filter staat vervolgens in het gedeelte op het scherm met de IP-adressen.

SNMP Password

Met behulp van het SNMP Password-scherm kunnen wijzigingen worden aangebracht in het SNMP-wachtwoord. Het wachtwoord wordt gebruikt voor de authenticatie van een SNMP-manager. Zodra deze is geauthenticeerd, worden configuratieverzoeken van de SNMP-manager gehonoreerd, zodat deze remote wijzigingen in de systeemconfiguratie mag aanbrengen.

Scherf 46: SNMP Password-scherm



Efficient NETWORKS

Current User: superuser

SNMP Password

This is the password used by all Client based Support applications such as Configuration Manager and Quick Start.

[SNMP Main Page](#)

[Home](#)

SNMP Password

Enter New Password:

New Password (again):

Apply

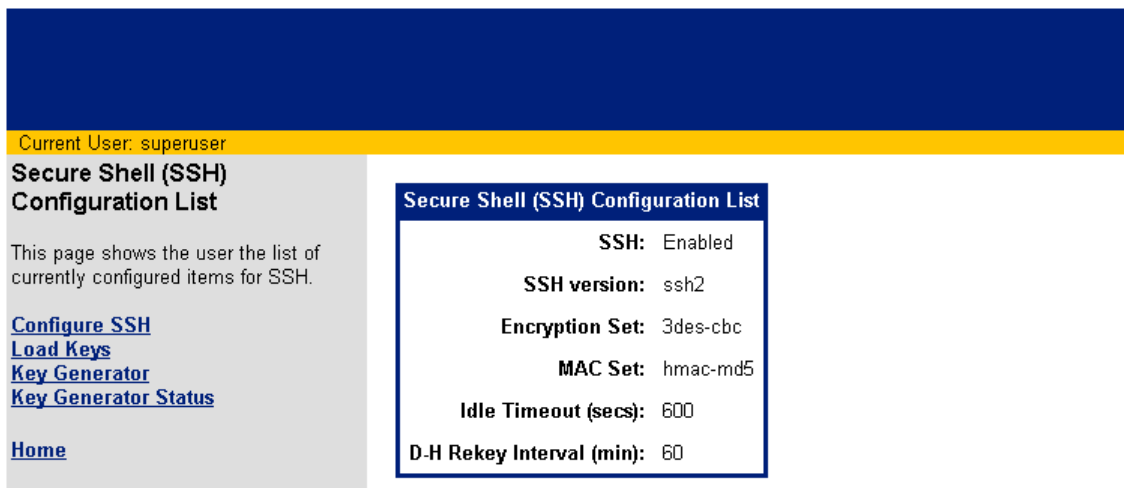
Voer de volgende stappen uit om het SNMP-wachtwoord te wijzigen:

- Stap 1:** Voer het nieuwe wachtwoord in het veld New Password in.
- Stap 2:** Ter bevestiging moet het nieuwe wachtwoord opnieuw in het veld New Password worden ingevoerd.
- Stap 3:** Klik op de knop Apply om uw nieuwe SNMP-wachtwoord in te stellen.

Secure Shell (SSH)

De Secure Shell (SSH) maakt de verzending mogelijk van veilige netwerkdiensten via een onveilig netwerk als het internet. SSH is een veilig en functioneel equivalent van Telnet. Telnet-verbindingen en -opdrachten staan een groot aantal compromissen toe, zoals het toestaan van een niet-geautoriseerde toegang, onderschepping en logging van verkeer van en naar het aangesloten systeem, inclusief wachtwoorden. SSH helpt deze veiligheidsmanco's en voorziet daarnaast in een veilige methode van bestandstransfers van het type FTP.

Scherf 47: Secure Shell (SSH) Configuration List-scherf



Het Secure Shell (SSH) Configuration List-scherf toont de bestaande SSH-configuratie-instellingen en voorziet in links met schermen voor de configuratie van de SSH en het maken van keys. Het Secure Shell (SSH) Configuration List-scherf toont de volgende informatie:

- SSH - Geeft aan of de SSH is in- (Enabled) of uitgeschakeld (Disabled).
- SSH Version - Geeft de versie weer van de in gebruik zijnde SSH.
- Encryption Set - Identificeert de in gebruik zijnde coderingsmethode.
- MAC Set - Identificeert het in gebruik zijnde type Message Authentication Code (MAC) voor de SSH-verbindingen.
- Idle Timeout (secs) - Geeft de interval aan (in seconden) gedurende welke een SSH-verbinding ongebruikt kan blijven voordat zij wordt verbroken.
- D-H Rekey Interval (min) - Geeft de interval (in minuten) aan waarop aanvullende key exchanges uitgevoerd zullen worden.

Links aan het linkerdeel van het scherm leiden naar de SSH-Configuration-schermen. Deze schermen worden hierna opgesomd en in de volgende gedeelten beschreven.

- [SSH configureren](#)
- [Load Keys](#)
- [Key Generator](#)
- [Key Generator Status](#)

Eerst moet een public/private key-paar naar de router worden geladen voor de SSH geconfigureerd kan worden. Als u nog geen keys in uw router hebt geladen/gemaakt, ga dan door met het gedeelte 'Load Private and Public Keys from file', volg de procedures voor het maken en/of laden van keys en keer vervolgens terug naar de SSH Configuration.

Configureer de Secure Shell (SSH)

Scherf 48: Configure Secure Shell (SSH)-scherm

Efficient NETWORKS

Current User: superuser

Configure Secure Shell (SSH)

This form allows the user to configure SSH.

[SSH Main Page](#)

[Home](#)

SSH Configuration

Status: ☒ Enable ☐ Disable

Encryption: ☐ DES ☒ 3DES ☐ ARC4
☐ Twofish ☐ Blowfish

MAC: ☒ MD5 ☐ SHA1

Port: ☐ Disable ☒ Default ☐ Port #:

Idle Timeout (secs):

D-H ReKey Interval (mins): ☐ No Retries

Het Configure Secure Shell (SSH)-scherm voorziet in instellingen voor de SSH van de router. De SSH Configuration omvat de volgende parameters:

- **Status** - Kan op Enable of Disable SSH worden gezet.
- **Encryption** - Beschrijft de geselecteerde coderingsmethode(n) voor de communicatie via de SSH. De geselecteerde methode is lokaal geconfigureerd op de router (of server). Als een client device met SSH-communicatie begint, wordt deze geïdentificeerd en in overeenstemming gebracht met de encryptiemethode van de server. Als een client zich niet aan de opgegeven codering houdt, komt er geen verbinding tot stand. U kunt meerdere encryptiemethoden tegelijkertijd kiezen, mits ze ondersteund worden.
- **MAC** - Beschrijft het type/de typen Message Authentication Code (MAC) van de SSH-verbindingen.
- **Port** - Geeft de poort aan die voor SSH wordt gebruikt, of stelt deze SSH-poort buiten werking.
- **Idle Timeout (sec.)** - Stelt de interval in (in sec.) en toont deze gedurende welke een SSH-verbinding ongebruikt mag blijven voordat zij wordt verbroken.
- **D-H Rekey Interval (min.)** - Stelt de interval in (in min.) van het uitvoeren van aanvullende key exchanges en toont deze.

Stap 1: Als op deze router nog geen key pair beschikbaar is, keer dan terug naar het scherm van de Secure Shell (SSH) Configuration List en maak daar een van de volgende procedures af om een key pair te laden of te maken (en dan te laden). Mocht er al een key pair in de router beschikbaar zijn, ga dan met de volgende stap door.

- [SSH Key Generation](#)
- [SSH Key Upload](#)

Stap 2: Stel de status in van de SSH door te klikken op de knop Enable of Disable.

Stap 3: Klik op de controlevakjes om een of meerdere encryptiemethoden te selecteren op de lijst.

Stap 4: Bepaal het type/de typen van MAC (Message Authentication Code) die u wilt gebruiken door te klikken op de controlevakjes.

Stap 5: Definieer de SSH Port door een van de volgende opties te kiezen:

- Deactiveer de SSH-poort door op de betreffende knop te klikken.
- Gebruik de standaard SSH-poort door op de betreffende knop te klikken.

- Gebruik een SSH Port# door op de betreffende knop te klikken en door het gewenste poortnummer in het betreffende veld in te voeren.

Stap 6: Voer de Idle Timeout (sec.) interval in het betreffende veld in. De interval kan een tijdsbestek zijn van 30 tot 1200 seconden. 600 seconden is de standaard Idle Timeout interval.

Stap 7: Voer de D-H ReKey Interval (in minuten) in het betreffende veld in. Deze interval kan een tijdsbestek zijn van 0 tot 600 seconden. De standaard ReKey Interval is 600 seconden. Optioneel kunt u ook op het controlevakje No Retries klikken om D-H ReKeying uit te schakelen gedurende de SSH-sessies. Als No Retries is aangekruist, zal er slechts aan het begin van de SSH-sessie een D-H key exchange optreden en de beginkeys in gebruik houden gedurende de gehele sessie. Gebruik deze optie als u verbindingen tot stand brengt met SSH-clients of servers die re-keying niet ondersteunen gedurende SSH-sessies.

Stap 8: Klik op de knop Apply om uw SSH-configuratie in te stellen en op te slaan.

Load Public and Private Keys

De SSH maakt en onderhoud verbindingen met behulp van een key exchange system, ook wel Diffie-Hellman genoemd. Dit exchange system vereist een public key en een private key. U kunt deze keys opvragen of door uw router laten maken. Als u al beschikt over een public en een private key pair, die u wilt gebruiken voor SSH, kunt u deze in de router laden met behulp van het scherm 'Load Public and Private Keys from file'. Het scherm is hieronder te zien.

Scherf 49: Load Public and Private Keys from File-scherf

De procedure voor het laden van public en private keys in uw router is als volgt:

Stap 1: Klik op de knop Public key of de knop Private key om een keytype te kiezen dat u wilt gaan uploaden.

Stap 2: Kies het keybestand dat u wilt uploaden op een van de volgende manieren:

- Typ het volledige pad in van het bestand in het veld Key File of -
- Klik op de knop Browse.... Navigeer naar de locatie van het keybestand en klik op Open of een vergelijkbare functie om de keuze van dit bestand te bevestigen.

Stap 3: Klik op de knop Upload om het keybestand te laden. U krijgt een bevestigingsmelding te zien zodra de upload is afgesloten.

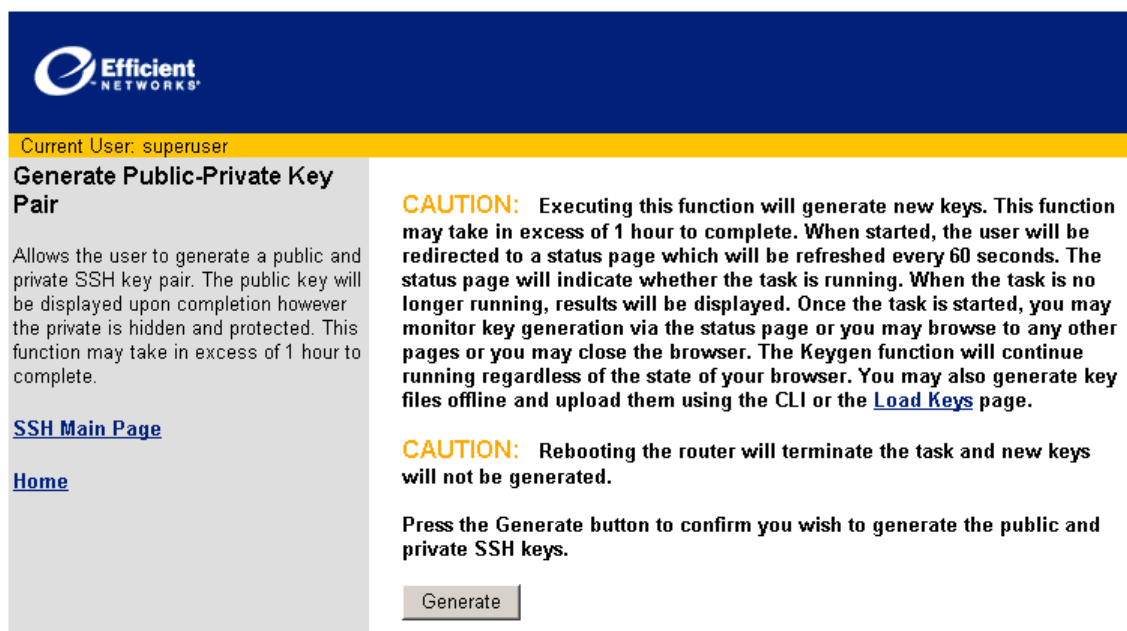
Stap 4: Herhaal deze procedure voor aanvullende keys die u in de router wilt laden. Om terug te keren naar het scherm Secure Shell (SSH) Configuration List moet u op de SSH Main Page-link klikken.

Key Generator

De SSH maakt en onderhoud verbindingen met behulp van een key exchange system, ook wel Diffie-Hellman genoemd. Dit exchange system vereist een public key en een private key. U kunt deze keys opvragen of door uw router laten maken. Als u een nieuw key pair wilt gebruiken voor de Secure Shell, kan de router

een nieuw pair voor uw maken in het scherm Generate Public-Private Key Pair. Het scherm is hieronder te zien.

Scherf 50: Generate Public-Private Key Pair-scherf



De procedure voor het maken van nieuwe public-private key pairs werkt als volgt:

Stap 1: Lees eerst de waarschuwing in het scherm van de Generate Public-Private Key Pair:



PAS OP! Door het uitvoeren van deze functie worden nieuwe keys gemaakt. De uitvoering van deze functie kan in sommige gevallen wel 1 uur duren. Na de start wordt de gebruiker teruggeleid naar een statuspagina die om de 60 seconden wordt geactualiseerd. De Status Page geeft aan of de task wordt uitgevoerd. Zodra de actie is afgelopen, zullen de resultaten worden weergegeven. Na het starten van de task kunt u hetzij het maken van de keys volgen via de statuspagina, hetzij naar een andere pagina gaan of u browser afsluiten. De Keygen-functie zet haar werkzaamheden voort, ongeacht de toestand van uw browser. U mag keybestanden ook offline maken om ze vervolgens te uploaden met behulp van de CLI- of Load Keys-pagina. PAS OP! Door het herstarten van uw router worden de lopende tasks geannuleerd en er geen nieuwe keys gemaakt.

Klik op de knop Generate als u het maken van public en private SSH keys wilt bevestigen.

Stap 2: Als u zeker weet dat u een SSH public-private key pair wilt maken, klik dan op de knop Generate.

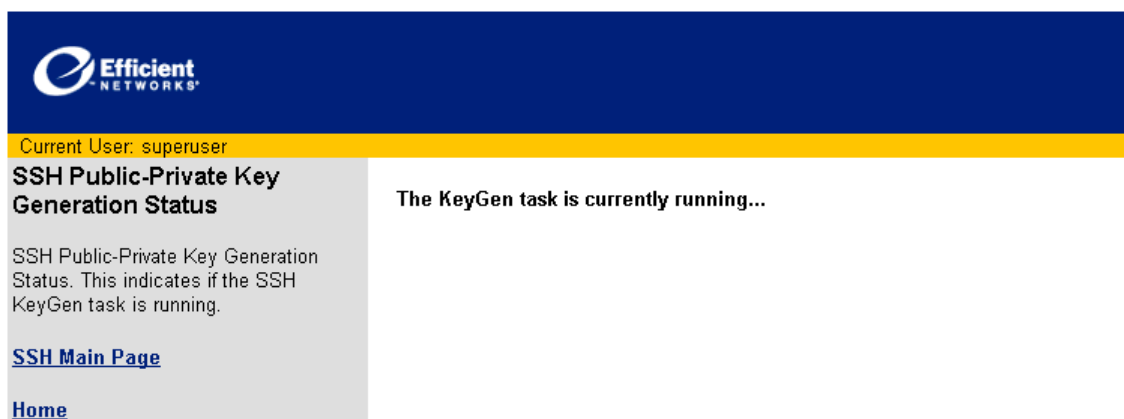
Stap 3: Om het maken van keys te kunnen volgen moet u op de Key Generator Status-link klikken in het scherm van de Secure Shell (SSH) Configuration List.

Opmerking: Gebruik alleen SSH Corporation key generation software om SSH keys offline mee te maken.

Key Generator Status

Het scherm SSH Key Generation Status verschijnt zodra een SSH key wordt gemaakt.

Scherf 51: SSH Key Generation Status-scherf



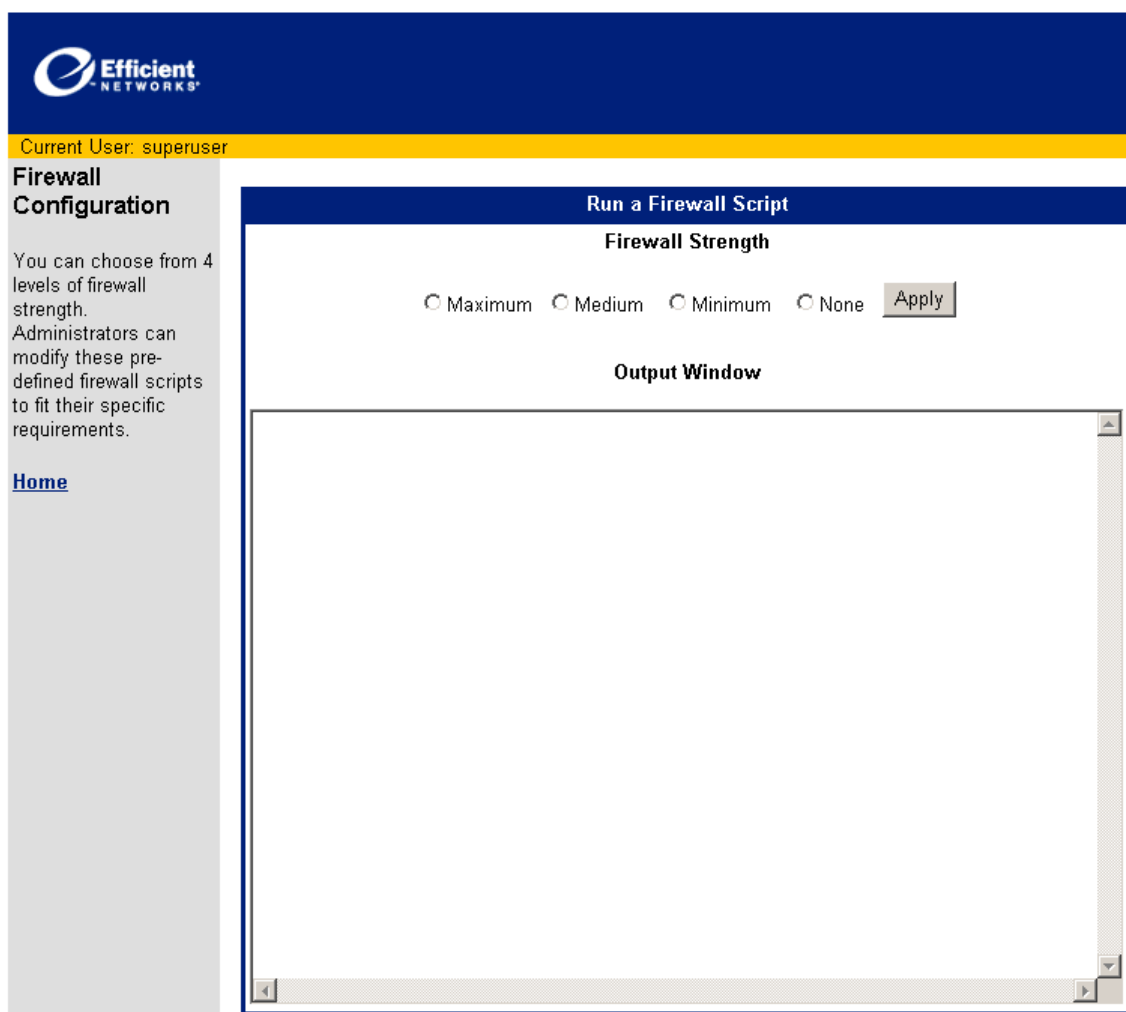
Om terug te keren naar het scherm Secure Shell (SSH) Configuration List moet u op de SSH Main Page-link klikken.

Klik op de link Home om terug te keren naar het scherm van de Router Information.

Firewall Configuration

Uw router beschermt uw netwerk en datacommunicatie met behulp van ingebouwde firewall-eigenschappen. Een firewall is elke combinatie van hardware en software dat een netwerk en het netwerkverkeer beschermt tegen wederrechtelijke onderbrekingen en inbraak. Uw router is voorzien van voorgedefinieerde scripts die aangepast kunnen worden of rechtstreeks kunnen worden gebruikt om firewalls te construeren.

Scherf 52: Firewall Configuration-scherf



Het Firewall-configuratiescherf wordt gebruikt voor het selecteren van een van de vier opties om een firewall op uw router in te stellen. De vier opties zijn:

- **Maximum** - Dit activeert een firewall met de meest restrictieve policy's voor een maximum aan veiligheid van uw netwerk.
- **Medium** - Dit activeert een firewall met flexibele policy's voor een gemiddeld niveau van netwerkbeveiliging.
- **Minimum** - Dit activeert een firewall met een basisset policy's voor een minimumniveau van netwerkbeveiliging.
- **None** - Geen firewall.

Voer de volgende stappen uit om uw firewall te activeren:

Stap 1: Klik op de knop naast de gekozen firewall-optie.

Stap 2: Klik op de knop Apply om uw firewall te activeren. Het Output Window toont de resultaten van de configuratie van uw firewall.

Stap 3: Klik op de knop Home om terug te keren naar het scherm Router Information.



PAS OP! Laat alle beveiligingsmaatregelen voor uw netwerk, inclusief de configuratie van uw firewall, uitvoeren door een ervaren en gekwalificeerde netwerkspecialist die vertrouwd is met de unieke architectuur en vereisten van uw netwerk. De fabrikant kan niet aansprakelijk worden gesteld voor ongeoorloofde indringing als gevolg van een ondeugdelijke of onjuiste configuratie van de firewall.

Quality of Service

Quality of Service (QoS) is een set van faciliteiten voor een actief management van netwerk bandbreedte om serviceniveaus voor prioritaire toepassingen te ondersteunen. Mission-critical en real-time netwerktoepassingen vereisen netwerkfaciliteiten die voorzien in veilige en stabiele netwerkdienstlevels en -bronnen. Quality of Service-faciliteiten voorzien in dit niveau van zekerheid. De volgende schermen omvatten configuratie- en managementopties voor de faciliteiten van de Quality of Service:

- [QoS Configuration](#)
- [QoS Policy-pagina](#)

QoS Configuration-scherm

Met het QoS-configuratiescherm kunt u de bestaande QoS-instellingen bekijken en configureren.

Scherm 53: QoS Configuration-scherm

Efficient NETWORKS

Current User: superuser

QoS Configuration

QoS Status
User can turn QoS on or off. In On mode, QoS will forward packets, set diffserv marking based on user defined mapping rules and QoS policies. In Off mode, QoS will forward packets based on pre-defined mapping rules and QoS settings.

DiffServ Status
User can turn diffserv on or off. In Off mode, QoS will not touch the IP header's DiffServ Marking. This is DiffServ pass through. In On mode, QoS will mark the DiffServ field according to the QoS Policies and pre-defined behavior.

QoS Priority/Weight Setting
User can setup values for 4 different priorities. The range of value is from 1 to 255. [Note: for Netscape users, you may need to click somewhere outside the field you just entered to get the percentage update to work]

[QoS Policy Page](#)

[Home](#)

Priority	Current Weight	New Weight	%
High	10	<input type="text" value="10"/>	
Medium	10	<input type="text" value="10"/>	
Normal	10	<input type="text" value="10"/>	
Low	10	<input type="text" value="10"/>	

Apply

De QoS-instellingen die in het QoS Configuration-scherm werden aangetroffen, zijn:

- **QoS Status** - Deze instelling zet de QoS-faciliteit aan (On) of uit (Off). De huidige instelling wordt weergegeven. Als deze faciliteit is ingeschakeld (ON), zal QoS de pakketten doorsturen en daarbij de diffserv tags markeren overeenkomstig de gebruikersspecifieke mapping rules en actieve QoS Policy's. Als QoS is uitgeschakeld (OFF), zal QoS de pakketten doorsturen overeenkomstig de voorge-definieerde mapping rules en instellingen van de QoS.
- **DiffServ Status** - Deze instelling zet de faciliteit DiffServ aan of uit. Als DiffServ is ingeschakeld (ON), zal QoS het DiffServ-veld markeren in de datapakketten overeenkomstig de QoS Policy's en de voorge-

- definieerde Mapping Rules. Als DiffServ is uitgeschakeld (OFF), zullen er geen tags verschijnen zodra er datapakketten passeren. Dit wordt ook wel 'DiffServ pass through' genoemd.
- QoS Priority/Weight Setting - Deze instellingen worden gebruikt om waarden toe te kennen voor max. vier verschillende prioriteiten. Deze voorkeuren hebben een numerieke waarde die tussen 0 en 256 ligt. Deze numerieke waarden voeren een rangschikking uit binnen de QoS m.b.t. de vier prioriteiten van het netwerkverkeer.

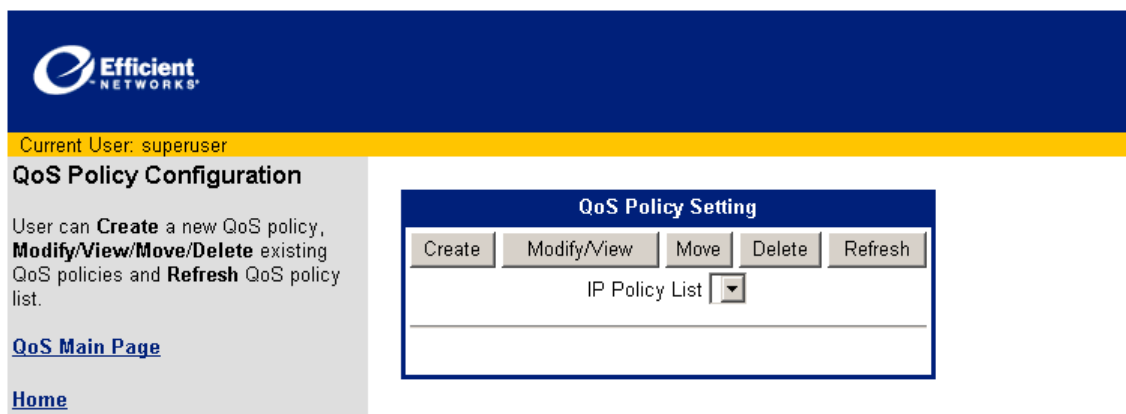
Voer de volgende stappen naar believen uit om de instellingen van de QoS Configuration te wijzigen.

- Stap 1:** Klik op een knop in de sectie QoS Status om QoS in of uit te schakelen.
- Stap 2:** Klik op een knop in de sectie DiffServ Status om DiffServ in of uit te schakelen.
- Stap 3:** Voer numerieke waarden in bij de vier velden van de QoS Priority/Weight Setting. De waarden liggen tussen 1 en 255.
- Stap 4:** Klik op de knop Apply om uw nieuwe QoS-instellingen in te stellen en op te slaan.

QoS Policy Configuration

Het QoS Policy Configuration-scherm voorziet in een menu met functies voor het management van QoS Policy's op de router.

Scherm 54: QoS Policy Configuration-scherm



De functies waarover het menu van de QoS Policy beschikt, zijn:

- [Maak](#) nieuwe QoS Policy's.
- [Wijzig/Bekijk](#) bestaandeg QoS Policy's.
- [Verschuif](#) QoS Policy's.
- [Verwijder](#) QoS Policy's.
- [Opfrissen](#) van de lijst van QoS Policy's. De QoS Policy List is een meerkeuzelijst onder de knop van de QoS Policy Setting.

De werkwijze van de functies wordt hierna beschreven.

Maak of wijzig een QoS Policy

Scherm 55: Create QoS Policy Configuration-scherm

Efficient NETWORKS

Current User: superuser

QoS Policy Configuration

User can **Create** a new QoS policy, **Modify/View/Move/Delete** existing QoS policies and **Refresh** QoS policy list.

[QoS Main Page](#)

[Home](#)

QoS Policy Setting

Create Modify/View Move Delete Refresh

IP Policy List ▼

Create

Policy Name

Status ☐ Enable ☒ Disable

Source IP ☐ From To ☒ Do not care

Dest IP ☐ From To ☒ Do not care

Protocol ☐ By number ☐ TCP ▼ ☒ Do not care

Source Port ☐ From To ☐ FTP ▼ ☒ Do not care

Dest Port ☐ From To ☐ FTP ▼ ☒ Do not care

Priority LOW ▼

Code Point - incoming ☐ ☒ Default

Code Point - outgoing ☐ ☒ Default

De volgende parameters worden gebruikt om een QoS Policy mee te maken of te wijzigen:

- Policy Name - Dit veld kent een naam toe aan een policy.
- Status - Met deze knoppen kan de QoS policy op Enable of Disable worden gezet.
- Source IP - Deze velden specificeren het bron-IP-adres of het bereik van IP-adressen die wordt/worden gecontroleerd door de QoS Policy. De knop 'Do not care' schakelt de controle uit van het bron-IP-adres.
- Dest IP - Dit veld geeft het doel-IP-adres aan of een reeks IP-adressen die door de QoS Policy wordt gecontroleerd. De knop 'Do not care' schakelt de controle uit van het doel-IP-adres.
- Protocol - Het veld By number geeft het protocol aan met behulp van zijn nummer. Via de meerkeuzelijst kunnen protocollen worden geselecteerd aan de hand van hun naam. De knop 'Do not care' schakelt de controle uit van het protocol.
- Source Port - Deze velden specificeren de bronpoort of het bereik van bronpoorten die wordt/worden gecontroleerd door de QoS Policy. Via de meerkeuzelijst kunnen de bronpoorten worden geselecteerd aan de hand van hun naam. De knop 'Do not care' schakelt de controle uit van de bronpoort.
- Dest Port - Dit veld geeft de doelpoort aan of een reeks poorten die door de QoS Policy wordt gecontroleerd. Via de meerkeuzelijst kunnen doelpoorten worden geselecteerd aan de hand van hun naam. De knop 'Do not care' schakelt de controle uit van de doelpoort.
- Priority - Deze lijst geeft de prioriteit aan van de QoS Policy. De standaardprioriteit is Normal.
- Code Point - incoming - Dit veld specificeert het inkomende codepunt voor de QoS Policy. De knop Standaard zet het inkomende codepunt op de standaardpositie.

- Code Point - outgoing - Dit veld specificeert de het uitgaande codepunt van de QoS Policy. De knop Standaard zet de uitgaande codepunt op de standaardpositie.
- Bidirection - Met deze knoppen kan de bidirectionele operatie van uw QoS-instellingen in- en uit worden geschakeld.
- Start Time - Specificeert het tijdsbestek gedurende de dag dat de QoS Policy actief is.
- Duration - Geeft het tijdsbestek aan waarbinnen de QoS policy actief moet blijven.
- Repetition - Specificeert de QoS Policy als: one-time, repeating of always-on.

Voer de volgende procedure uit om een QoS Policy te maken of te wijzigen:

Stap 1: Vul de velden in en kies de opties voor uw QoS policy.

Stap 2: Klik op de knop Apply om uw QoS policy op te slaan.

Een QoS Policy verschuiven

Scherf 56: Move QoS Policy-scherf

The screenshot displays the 'QoS Policy Configuration' page of the Efficient Networks management interface. The top header is blue with the 'Efficient NETWORKS' logo. Below it, a yellow bar indicates the 'Current User: superuser'. The left sidebar contains links for 'QoS Main Page' and 'Home'. The main content area is titled 'QoS Policy Setting' and features a row of buttons: 'Create', 'Modify/View', 'Move', 'Delete', and 'Refresh'. Below these buttons is a dropdown menu labeled 'IP Policy List'. The 'Move' section is active, showing a 'Policy' text input field, two radio button options: 'to the end' and 'before policy', and a corresponding text input field for the 'before policy' option. At the bottom of this section are 'Apply' and 'Cancel' buttons.

De Move-optie van de QoS Policy Configuration voorziet in velden die nodig zijn om QoS Policy's op de QoS Policy List te verschuiven. QoS policies worden uitgevoerd in afdalende volgorde van deze lijst. Om een QoS Policy te verschuiven, moet u de volgende stappen uitvoeren:

Stap 1: Geef in het veld Policy de naam op van de QoS Policy die u wilt gaan verschuiven.

Stap 2: Kies een knop om de QoS Policy naar het einde van de lijst ('to the end') te verschuiven of naar 'before policy'. Voer de naam van de QoS Policy die voorrang heeft in het betreffende veld in.

Stap 3: Klik op de knop Apply om uw nieuwe lijstvolgorde op te slaan. U kunt ook op de knop Cancel klikken om uw QoS-invoer ongedaan te maken.

Verwijder een QoS Policy

Scherf 57: Delete QoS Policy-scherf

The screenshot displays the Efficient Networks QoS Policy Configuration interface. On the left, a sidebar shows the 'Current User: superuser' and a list of actions: 'Create', 'Modify/View/Move/Delete', and 'Refresh'. Below this, there are links for 'QoS Main Page' and 'Home'. The main content area is titled 'QoS Policy Setting' and contains a 'Delete' dialog. The dialog has a title bar 'QoS Policy Setting' and buttons for 'Create', 'Modify/View', 'Move', 'Delete', and 'Refresh'. Below the buttons is a dropdown menu labeled 'IP Policy List'. The 'Delete' section of the dialog contains two radio button options: 'all policies in IP policy list' and 'policy'. The 'policy' option is selected, and there is a text input field next to it. At the bottom of the dialog are 'Apply' and 'Cancel' buttons.

De Delete-optie van de QoS Policy Configuration voorziet in velden die nodig zijn om een policy of alle policy's van een QoS te verwijderen van de IP Policy list. Voer de volgende procedure uit om een IP Policy of meerdere IP policy's te verwijderen:

- Stap 1:** Klik op een van de radioknoppen om 'all policies in IP policy list' te verwijderen of een heel bepaalde policy.
- Stap 2:** Als u een heel bepaalde policy wilt verwijderen, voer dan in het betreffende veld de naam van deze policy in.
- Stap 3:** Klik op de knop Apply om het verwijderen van de policy af te sluiten. U kunt ook op de knop Cancel klikken om het wissen van uw policy af te breken.

Fris de QoS Policy Configuration op.

Om het QoS Policy Configuration-scherf te actualiseren, klikt u de knop Refresh.

Stateful Firewall

Traditionele firewalls zijn stateless. Met andere woorden: ze hebben geen geheugen waarin de verbindingen zijn opgeslagen van de datapakketten die de firewall zijn gepasseerd. Zulke IP filterende firewalls controleren de header-informatie van elk pakket en vergelijken deze met een set van gedefinieerde regels. Als de firewall overeenstemming aantreft, wordt de beschreven actie uitgevoerd. Als er geen overeenstemming vastgesteld kon worden, zal het pakket in het netwerk alnaargelang de configuratie van de firewall worden geaccepteerd of afgewezen.

Een Stateful Firewall bevat een geheugen waarin alle verbindingen en gegevens die door de firewall zijn gegaan, zijn opgeslagen. Stateful firewalls registreren de context van de verbindingen gedurende elke sessie door een voortdurende update van de toestandsgegevens in dynamische tabellen. Met deze informatie controleren Stateful Firewalls elke verbinding die de interface van de firewall over en weer passeert door de pakketten gedurende de gehele sessie op hun geldigheid te testen. Zodra data binnenkomen, worden deze met de tabellen vergeleken; maken de data deel uit van de sessie, dan worden ze geaccepteerd. Stateful Firewalls maakt een intelligentere, meer flexibele en robuustere benadering mogelijk van netwerkbeveiliging door beter te zijn dan de afweermethoden van de stateless IP filterende firewalls.

Stateful Firewall Configuration-scherm

Het Stateful Firewall Configuration-scherm stelt u in staat om de bestaande firewallinstellingen te bekijken en te configureren. Voorziet tevens in links met de pagina met afgewezen pakketten en die van de Firewall Rule.

Scherm 58: Stateful Firewall Configuration-scherm

Efficient NETWORKS

Current User: superuser

Stateful Firewall Configuration

Firewall Status
User can turn the firewall on/off.

Watch Setting
If watch is turned on, the messages are printed to the console whenever a packet is accepted or dropped.

Dropped Packet Threshold Setting
When the number of dropped packets exceeds the threshold value, the firewall will log a message to the console. Default value is 200 per second.

UDP Packet Threshold Setting
The firewall would block any subsequent UDP packets by default if the counter for the UDP packets exceeds the threshold value. Default value is 1000 per second.

ICMP Ping Packet Threshold Setting
The firewall would block any subsequent

Firewall Status
☐ On
☒ Off **Current Setting**

Watch Setting
☐ On
☒ Off **Current Setting**

Dropped Packet Threshold Setting
Current: 200 New:

UDP Packet Threshold Setting
Current: 1000 New:

ICMP Ping Packet Threshold Setting
Current: 1000 New:

SYN Packet Threshold Setting
Current: 200 New:

Apply

De instellingen van het Stateful Firewall Configuration-scherm zijn:

- Firewall Status - Deze geeft aan of de firewall is in- of uitgeschakeld.
- Watch Setting - Dit geeft aan of de Watch Setting is in- of uitgeschakeld. Als de Watch Setting is ingeschakeld (ON), wordt er een melding afgedrukt zodra een pakket is geaccepteerd of afgewezen.
- Dropped Packet Threshold Setting - Zodra het aantal afgewezen pakketten deze drempelwaarde overschrijdt, stuurt de firewall een melding naar de console. De standaarddrempelwaarde is 200.

- UDP Packet Threshold Setting - Zodra een UDP-pakket teller deze drempelwaarde overschrijdt, zal de firewall dit UDP-pakket afwijzen. De standaarddrempelwaarde is 1000 per seconde.
- ICMP Ping Packet Threshold Setting - Zodra de ICMP ping pakket teller deze drempelwaarde overschrijdt, zal de firewall alle ICMP ping pakketten afwijzen. De standaarddrempelwaarde is 1000 per seconde.
- SYN Packet Threshold Setting - Zodra de SYN-pakket teller voor een bepaald doel de drempelwaarde overschrijdt, zal de firewall alle aanvragen van SYN afwijzen die voor dit doel bestemd zijn. De standaarddrempelwaarde is 200 per seconde.

Om de instellingen van de Stateful Firewall Configuration overeenkomstig uw wensen te wijzigen, moet u de volgende stappen uitvoeren:

- Stap 1:** Klik op een knop Firewall Status om deze instelling in of uit te schakelen.
- Stap 2:** Klik op een knop Watch Setting om deze instelling in of uit te schakelen.
- Stap 3:** Voer geheel naar wens nieuwe waarden in het veld Threshold Setting in.
- Stap 4:** Klik op de knop Apply om uw nieuwe configuratie op te slaan.

Dropped Packet List

Het Dropped Packet List-venster toont een recentelijk overzicht van afgewezen pakketten, inclusief details over deze pakketten. U kunt de laatste 200 afgewezen pakketten op de lijst bekijken.

Het Dropped Packet List-scherm is hieronder te zien.

Scherf 59: Dropped Packet List-scherm

Efficient NETWORKS

Current User: superuser

Dropped Packet List

This allows the user to view the last few dropped packets. The user can view up to 200 dropped packets. [Note: for Netscape 4 users, you may have to wait for a very long time to get the list displayed. Please select a smaller value]

[Firewall Main Page](#)

[Home](#)

Firewall Dropped Packet List

How many packets do you want to see?

(1-200)

☒ Default (200 packets)

#	Date	Time	Protocol	Source IP	Src Port/ ICMP Type	Destination IP	Dst Port/ ICMP Code	Reason
---	------	------	----------	-----------	------------------------	----------------	------------------------	--------

U kunt de lijst van afgewezen pakketten bekijken door de volgende stappen uit te voeren:

- Stap 1:** Kies het aantal afgewezen pakketten die u wilt zien met behulp van een van de twee methoden:
- Klik op de bovenste knop om het aantal pakketten in te voeren dat u wilt gaan bekijken. Voer het nummer in het aangrenzende veld in. Dit getal moet liggen tussen 1 -200, inclusief, of -
 - Klik op onderste knop om het standaard aantal pakketten in te stellen die weergegeven worden. Het standaard aantal pakketten is 200.
- Stap 2:** Klik op de knop Apply. De lijst van afgewezen pakketten (dropped packets) wordt weergegeven.

Opmerking: Netscape 4 en oudere browsers zullen lang doen over het laden van deze lijst. Laat niet al te grote pakketten weergeven als u nog met een oudere browser werkt.

Stateful Firewall Rule-configuratie

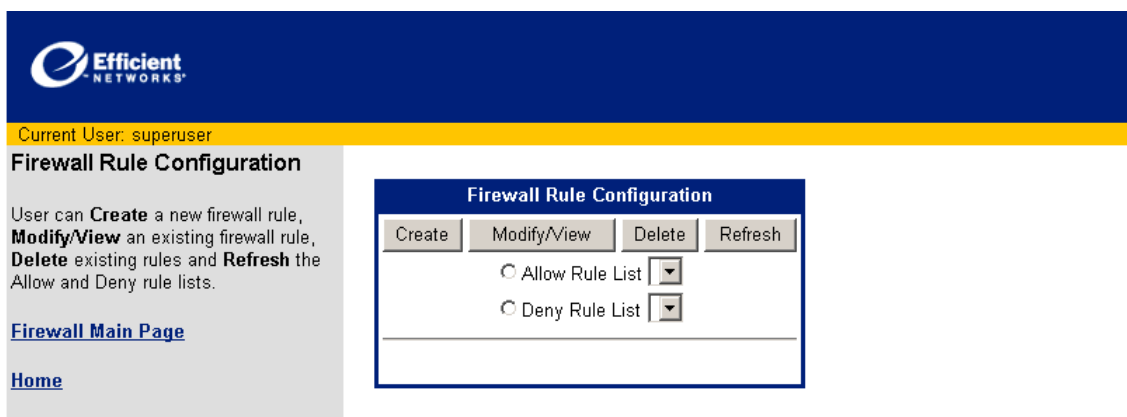
Als een firewall, voert de stateful firewall beveiligingsacties uit voor uw netwerk die zijn gebaseerd op de regels die uw netwerkbeheerder heeft gedefinieerd. Deze regels voorzien de Stateful Firewall met een richtsnoer voor het efficiënte managen van verbindingen en data, terwijl tevens adequaat wordt gereageerd op bedreigingen voor de netwerkveiligheid. Er bestaan twee hoofdtypen van deze regels: Allow of Deny. Zodra een pakket wordt geëvalueerd, worden eerst de Deny Rules toegepast en dan de Allow Rules. Dit pakket moet voldoen aan een reeks criteria, die in de regel worden vastgelegd vóór de regel wordt toegepast op het pakket.

Het Stateful Firewall Rule Configuration-schermbord voorziet in bedienopties voor het managen van de regels van uw Stateful Firewall. Deze bedienopties staan in een menu dat u in staat stelt om:

- [Maak](#) nieuw firewall-regels
- [Wijzig of bekijk](#) bestaande regels
- [Verwijder](#) bestaande regels
- [Opfrissen](#) van de lijsten Allow en Deny Rule

Het Stateful Firewall Rule Configuration-schermbord is hieronder te zien.

Schermbord 60: Stateful Firewall Rule Configuration-schermbord



Voor toegang tot de firewall-regels, moet u de volgende stappen uitvoeren:

- Stap 1:** Klik op een van de vier menuknoppen boven in het venster van de Firewall Rule Configuration om het scherm weer te geven van de betreffende actie.
- Stap 2:** Klik op de knop Allow Rule List of de knop Deny Rule List en kies een regel uit de weergegeven meerkeuzelijst.

Stateful Firewall Rules maken

De Create Mode van het scherm Stateful Firewall Rule Configuration toont de bedienopties voor het maken van nieuwe firewall-regels.

Scherf 61: Create Stateful Firewall Rule-scherf

Stateful Firewall Rule Parameters

Met de volgende parameters kunnen Stateful Firewall Rules worden gemaakt en gewijzigd:

- Rule List - Voor firewall-regels; er bestaan twee soorten: Allow Rules en Deny Rules. Allow Rules geven de voorwaarden aan onder welke datapakketten de firewall over en weer mogen passeren. Deny Rules specificeren de voorwaarden onder welke pakketten worden afgewezen. Zodra een pakket wordt geëvalueerd, zullen eerst de Deny Rules worden toegepast en daarna de Allow Rules.
- Protocol/Port - Als Protocol/Port is geactiveerd, kunnen hier nog aanvullende criteria worden ingesteld waaraan een pakket moet voldoen voor het op een firewall-rule stoot. Naast de bron (Source) en het doel (Destination) van het protocol kunnen ook aanvullende criteria worden opgegeven waaraan het pakket moet voldoen. Als er slechts één bronpoort is opgegeven, moet het pakket precies in overeenstemming zijn met de poort. Als er een bereik van poorten is gedefinieerd, moet de bronpoort van het pakket hiermee corresponderen. Als er geen poort is opgegeven, zal de regel elke bronpoort toelaten binnen een bereik van 0-65535. U kunt kiezen tussen vier beschikbare protocols:
- TCP - Transport Control Protocol
- UDP - User Datagram Protocol

- **Number** - Dit veld geeft het protocol met behulp van het nummer.
- **ICMP** - Internet Control Message Protocol - Als het protocol ICMP is, moet de bron van het pakket met het opgegeven ICMP-type corresponderen. Het ICMP-pakket moet corresponderen met de ICMP-code.
- **Application** - Dit veld wordt gebruikt om een toepassing als doel van een regel te definiëren.
- **Address** - Aan de hand van deze parameters worden de grenzen van het bron- en doel-IP adres gedefinieerd die van toepassing zijn op de firewall rule.
- **Source/Destination IP Address** - Het pakket moet een bron- of doel-IP-adres hebben dat binnen het opgegeven adresbereik ligt. Als er slechts één adresbereik is opgegeven, moet het pakket in ieder geval hetzelfde bron- of doel-IP-adres hebben. Als er geen bron- of doel-IP-adres is opgegeven, geldt de firewall-regel voor elk geldig IPv4- adres.
- **Source/Destination Mask** - De firewall-regel gebruikt dit bepaalde masker om het bron- of doel-IP-adres te vergelijken met het IP-adres van het datapakket. Als er geen masker is gespecificeerd, heeft deze de waarde 255.255.255.255.
- **Mode** - De Mode geeft aan wanneer watch-meldingen getoond zullen worden naar aanleiding van de firewall-regel. De Watch Messages worden naar de seriële poort van de console gestuurd en naar de Syslog-server, mits zodanig geconfigureerd. De modusopties zijn:
 - **Quiet** - Deze modus stuurt geen Watch Messages van deze firewall-regel. Dit geldt ook als de regel een datapakket afwijst. Dit is de standaardinstelling voor de Allow Rules van de firewall.
 - **Verbose** - Deze modus stuurt een Watch Message zodra de firewall-regel correspondeert met een datapakket, ongeacht de aansluitende actie.
- **Direction** - Deze parameter geeft de richting aan van het netwerkverkeer waarvoor de firewall-regel van toepassing is. Der standaardrichting is beide.

Om een nieuwe Stateful Firewall-regel te maken, moet u de volgende stappen uitvoeren:

Stap 1: Klik hier om de Rule List te kiezen waaraan u nieuwe firewall-regels gaat toevoegen:

- Allow Rule List
- Deny Rule List

Stap 2: Klik op de knop Create om de bedienopties van de Firewall Rule Configuration weer te geven.

Stap 3: Configureer de parameters overeenkomstig de vereisten voor deze regel. Voor nadere informatie over deze parameters, zie het vorige gedeelte.

Stap 4: Klik op de knop Save om uw nieuwe firewall-regel op te slaan in de geselecteerde regellijst.



***PAS OP!** Laat alle beveiligingsmaatregelen voor uw netwerk, inclusief de configuratie van uw firewall, uitvoeren door een ervaren en gekwalificeerde netwerkspecialist die vertrouwd is met de unieke architectuur en vereisten van uw netwerk. De fabrikant kan niet aansprakelijk worden gesteld voor ongeoorloofde indringing als gevolg van een ondeugdelijke of onjuiste configuratie van de firewall.*

Wijzig/Bekijk Stateful Firewall Rules

Om een bestaande firewall-regel te wijzigen of te bekijken, moet u de volgende stappen uitvoeren:

Stap 1: Kies de firewall-regel die u wilt wijzigen uit de Allow Rule List of de Deny Rule List.

Stap 2: Klik op de knop Modify/View. Nu wordt de firewall-regel weergegeven.

Stap 3: Breng naar believen wijzigingen aan in de firewall-regel.

Stap 4: Klik op de knop Save om uw wijzigingen te bevestigen van de firewall-regel. Klik op de knop Cancel om de rule view af te sluiten zonder de wijzigingen op te slaan.

Stateful Firewall Rules verwijderen

De Delete Mode in het scherm van de Stateful Firewall Rule Configuration toont de bedienopties voor het verwijderen van firewall-regels. Het scherm is hieronder te zien.

Scherf 62: Delete Stateful Firewall Rule-scherf

The screenshot shows the 'Efficient NETWORKS' logo at the top left. Below it, a yellow bar indicates 'Current User: superuser'. The main title is 'Firewall Rule Configuration'. On the left sidebar, there is a description: 'User can **Create** a new firewall rule, **Modify/View** an existing firewall rule, **Delete** existing rules and **Refresh** the Allow and Deny rule lists.' Below this are links for 'Firewall Main Page' and 'Home'. The main panel has a header 'Firewall Rule Configuration' with buttons 'Create', 'Modify/View', 'Delete', and 'Refresh'. Below these are radio buttons for 'Allow Rule List' and 'Deny Rule List'. The 'Delete' section contains four options: 'all rules in allow list', 'all rules in deny list', 'all rules in allow list and deny list', and 'rule number from [] to [] in [Allow]'. At the bottom are 'Apply' and 'Cancel' buttons.

Voer de volgende procedure uit om een firewall-regel te verwijderen:

- Stap 1:** Klik op de knop Delete in het menu van de Firewall Rule Configuration.
- Stap 2:** Klik hier om de Rule List te kiezen van welke u de firewall-regels gaat verwijderen.
- Stap 3:** Klik onder het deel Delete in het scherm op een van de volgende verwijderknoppen:
- Alle regels van de Allow List - Met deze optie worden alle firewall-regels van de Allow List verwijderd.
 - Alle regels van de Deny List - Met deze optie worden alle firewall-regels van de Deny List verwijderd.
 - Alle regels van de Allow List en de Deny List - Met deze optie worden alle firewall-regels van zowel de Deny List als de Allow List verwijderd.
 - Regelnummer van...tot...in... - Deze optie verwijdert slechts één regel of alle regels van de betreffende lijst in het opgegeven bereik.
1. Voer de firewall-regel in het eerste veld (from) in of voer de eerste regel van een reeks van regels in die u wilt gaan verwijderen. Als er slechts één regel is ingesteld, ga dan door met stap drie.
 2. Voer in het tweede veld (to) de laatste firewall-regel in van de reeks regels die u wilt gaan verwijderen.
 3. Kies de Rule List uit het meerkeuzemenu die de firewall-regel bevat die u wilt verwijderen.

Opmerking: Als een bereik van firewall-regels is bedoeld om verwijderd te worden, horen hier altijd ook de eerste en de laatste regel bij.

- Stap 4:** Klik op de knop Apply om het verwijderen van firewall-regels af te sluiten. U kunt ook op de knop Cancel klikken om het wissen af te breken.

Actualiseer Stateful Firewall Rules

De Refresh Mode in het scherm van de Stateful Firewall Rule Configuration toont een geactualiseerde lijst van de bestaande en geconfigureerde firewall-regels. Om de lijst van firewall-regels op te frissen, moet u de volgende stappen uitvoeren.

Stap 1: Klik op de knop Refresh in het scherm van de Firewall Rule Configuration. Het venster van de Firewall Rule Configuration verschijnt, inclusief de geactualiseerde lijsten.

Dial Backup

Dial Backup voorziet in een backup-verbinding met uw serviceprovider via een modem. Deze backup-link kan geactiveerd worden in het geval van een storing of onderbreking van uw eerste WAN-dienst. Gedurende zulke onderbrekingen zal uw router de Dialup-modemverbinding gebruiken terwijl de primary WAN-dienst wordt hersteld. Zodra de eerste netwerklink weer actief is, schakelt de Dial Backup automatisch over naar de eerste netwerkverbinding. De dienst Voice is uitgeschakeld gedurende de Dial Backup.

Het Dial Backup-scherm is hieronder te zien.

Scherf 63: Dial Backup Setup-scherm

Efficient NETWORKS

Current User: superuser

Dial Backup

Use the console (serial) port to attach an external analog modem. To use the dial backup function, users must enable it first.

[Home](#)

☐ Enable Dial Backup

User name

Password

Phone number

Alternative Phone number (optional)

☒ Disable Dial Backup

Apply

Voer de volgende stappen uit om Dial Backup te configureren:

- Stap 1:** Klik op de knop Enable Dial Backup.
- Stap 2:** Voer uw gebruikersnaam, die u van uw netwerkprovider hebt ontvangen, in het veld User Name in.
- Stap 3:** Voer uw wachtwoord, dat u van uw netwerkprovider hebt ontvangen, in het veld Password in.
- Stap 4:** Voer het eerste telefoonnummer in het betreffende veld in voor de dial-up-toegang tot uw netwerkprovider.
- Stap 5:** Optioneel kunt u ook een ander telefoonnummer in het betreffende veld invoeren voor de dial-up-toegang tot uw netwerkprovider.
- Stap 6:** Klik op de knop Apply om uw Dial Backup-configuratie te activeren. Het Dial Backup-configuratiescherm verschijnt
- Stap 7:** Voer de waarde van de Backup Failover Timeout (in minuten) in het betreffende veld in. Deze instelling definieert een tijdsinterval waarmee buitensporig heen-en-weer-schakelen wordt voorkomen tussen de WAN-link en de backup-poort. De standaard Failover-periode is drie minuten.
- Stap 8:** Voer de waarde van de Reset WAN Timer (in minuten) in het betreffende veld in. Deze timer geeft de interval aan tussen de controlepunten om vast te stellen of de WAN-link weer hersteld is.

- Stap 9:** Voer de IP-adressen in het veld IP Addresses in. De IP-adressen zijn die adressen die de router gebruikt om een ping uit te voeren via de WAN-link. Als de ping-test is mislukt, zal de router het verkeer via de backup-poort afwerken totdat de tijd voor herhalingen is afgelopen.
- Stap 10:** Voer de Ping Success Rate in het betreffende veld in. Het resultaat van ping (Ping Success Rate) is van toepassing op alle adressen die zijn opgegeven in het veld IP Addresses. Zodra het resultaat van alle succesvolle pings (m.b.t. alle IP-adressen) onder de Ping Success Rate komt te liggen, wordt verondersteld dat de WAN-link geen verbinding tot stand kan brengen; de router schakelt over op Dial Backup.
- Stap 11:** Klik om de Modem Dial String te kiezen. De Modem Dial String maakt gebruik van de geschikste modem dial string voor de interne modem, gebaseerd op het type verbinding dat u hebt geselecteerd.
- Stap 12:** Klik op de knoppen Save en Reboot om uw Dial Backup-instellingen op te slaan en te activeren. Uw router zal een herstart uitvoeren met de nieuwe Dial Backup Configuration.

ATM Traffic Shaping Configuration

Het scherm Traffic Shaping Configuration voorziet in bedienopties voor het managen van de ATM-25 link met uw router. Het ATM Traffic Shaping Configuration-scherm is hieronder te zien.

Scherf 64: ATM Traffic Shaping Configuration-scherm

Efficient NETWORKS

Current User: superuser

ATM Traffic Shaping Configuration

Please select from one of the following service types:

Constant Bit Rate
Specifies a fixed bit rate so that data is sent in a steady stream. A PCR setting is required.

Real-Time Variable Bit Rate
Provides a specified throughput capacity but data is not sent evenly. PCR, SCR and MBS settings are required.

Non-Real-Time Variable Bit Rate
Provides a specified throughput capacity but data is not sent evenly. Delay is expected with this setting. PCR, SCR and MBS settings are required.

Unspecified Bit Rate
Does not guarantee any throughput levels. A PCR setting is required.

[Home](#)

ATM Traffic Shaping Configuration

Please select an interface

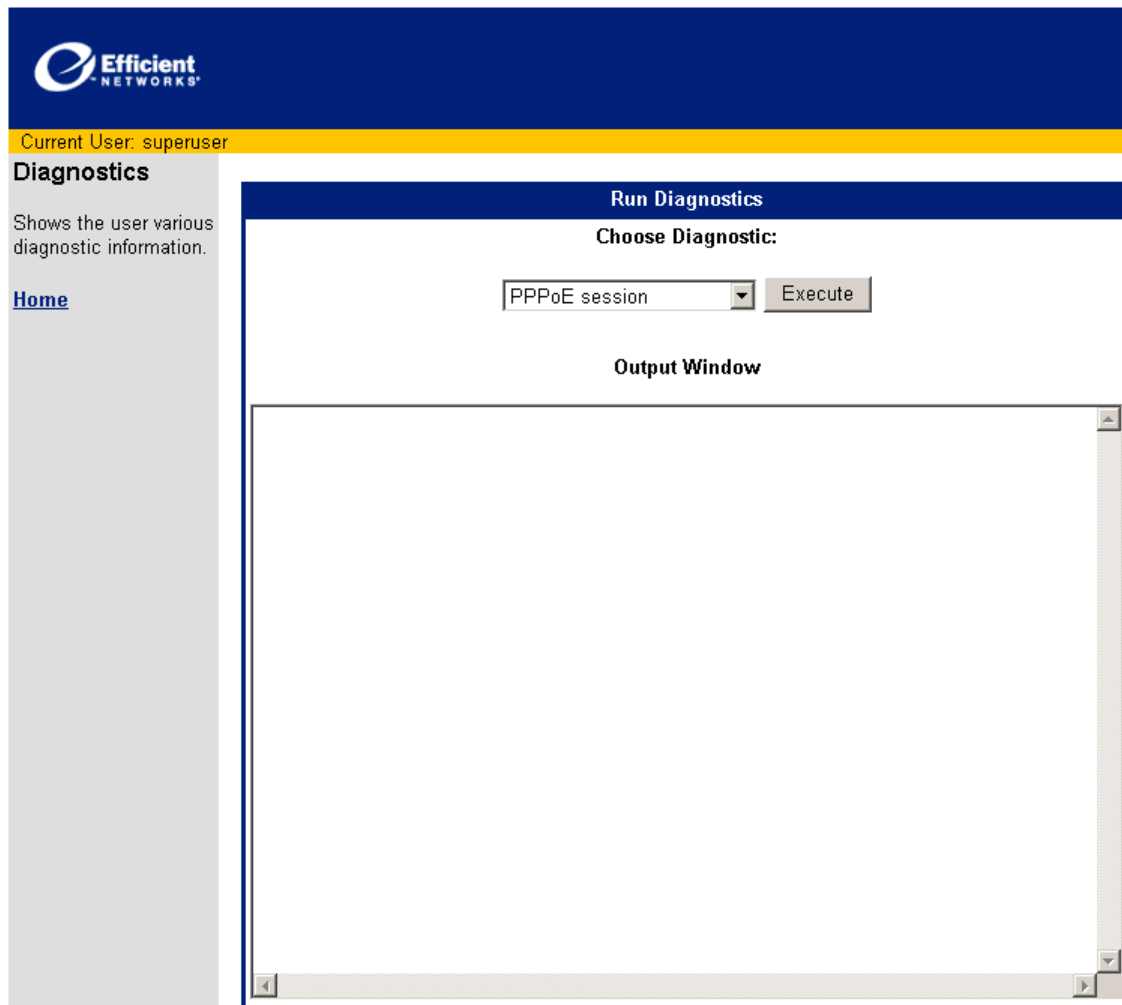
De configuratie van ATM kan worden uitgebreid door de volgende stappen uit te voeren:

- Stap 1:** Kies in het scherm ATM Traffic Shaping Configuration een interface uit de betreffende lijst. In de meeste gevallen moet u 'internet' kiezen.
- Stap 2:** De opties van de ATM Traffic Shaping Configuration van de door u gekozen interface verschijnen. Klik op de aangrenzende knop om een van de onderstaande typen ATM-diensten:
- **Constant Bit Rate** - Deze faciliteit voorziet in een constante, uniforme transmissiesnelheid. Deze dienst vereist een Peak Cell Rate (PCR) parameterwaarde. Voer de waarde in het betreffende veld in.
 - **Real-Time Variable Bit Rate** - Deze dienst voorziet in transmissiesnelheden die variëren binnen van te voren bepaalde limieten. Deze faciliteit vereist invoeren voor Peak Cell Rate (PCR), Sustained Cell Rate (SCR) en Maximum Burst Size (MBS). Voer deze waarden in de betreffende velden in.
 - **Non-Real-Time Variable Bit Rate** - Deze dienst voorziet in een transmissiesnelheid die varieert binnen van te voren bepaalde limieten. Bij dit soort diensten kunnen vertragingen ontstaan. Deze faciliteit vereist invoeren voor Peak Cell Rate (PCR), Sustained Cell Rate (SCR) en Maximum Burst Size (MBS). Voer deze waarden in de betreffende velden in.
 - **Unspecified Bit Rate** - Deze faciliteit geeft geen throughput-levels weer. Deze dienst vereist een Peak Cell Rate (PCR) parameterwaarde. Voer de waarde in het betreffende veld in.
- Stap 3:** Klik op Apply om de configuratie op te slaan en terug te keren naar het scherm Router Information. U kunt ook op de knop Select Another Interface klikken als u een andere ATM-verkeersverbinding wilt configureren.

Diagnostic

Het Diagnostics-schermbord voorziet in diagnosetesten en controleert de status van diverse routersystemen. U kunt de tests via een meerkeuzemenu selecteren en uitvoeren. De resultaten van de tests zijn te zien in de Output Window.

Schermbord 65: Diagnostics-schermbord



Om een diagnosetest via het Diagnostics-schermbord te starten, moet u de volgende stappen uitvoeren:

- Stap 1:** Kies een test uit de meerkeuzelijst van Choose a Diagnostic.
- Stap 2:** Klik op de knop Execute om de diagnose uit te voeren. U kunt de resultaten bekijken in het outputvenster.

Command Line Interface

Het scherm Command Line Interface voorziet in een faciliteit voor het invoeren van commando's voor de router via de web-gebruikersinterface.

Een volledig overzicht van alle router-commando's treft u aan in de Command Line Interface Reference Guide, te vinden op uw programma-cd. Het scherm Command Line Interface is hieronder te zien.

Scherf 66: Command Line Interface-scherf

Efficient NETWORKS

Current User: superuser

Web Gateway to Command Line Interface

Allows the user to enter any CLI command over the web interface.

[Home](#)

Execute a CLI command

CLI command:

Output Window

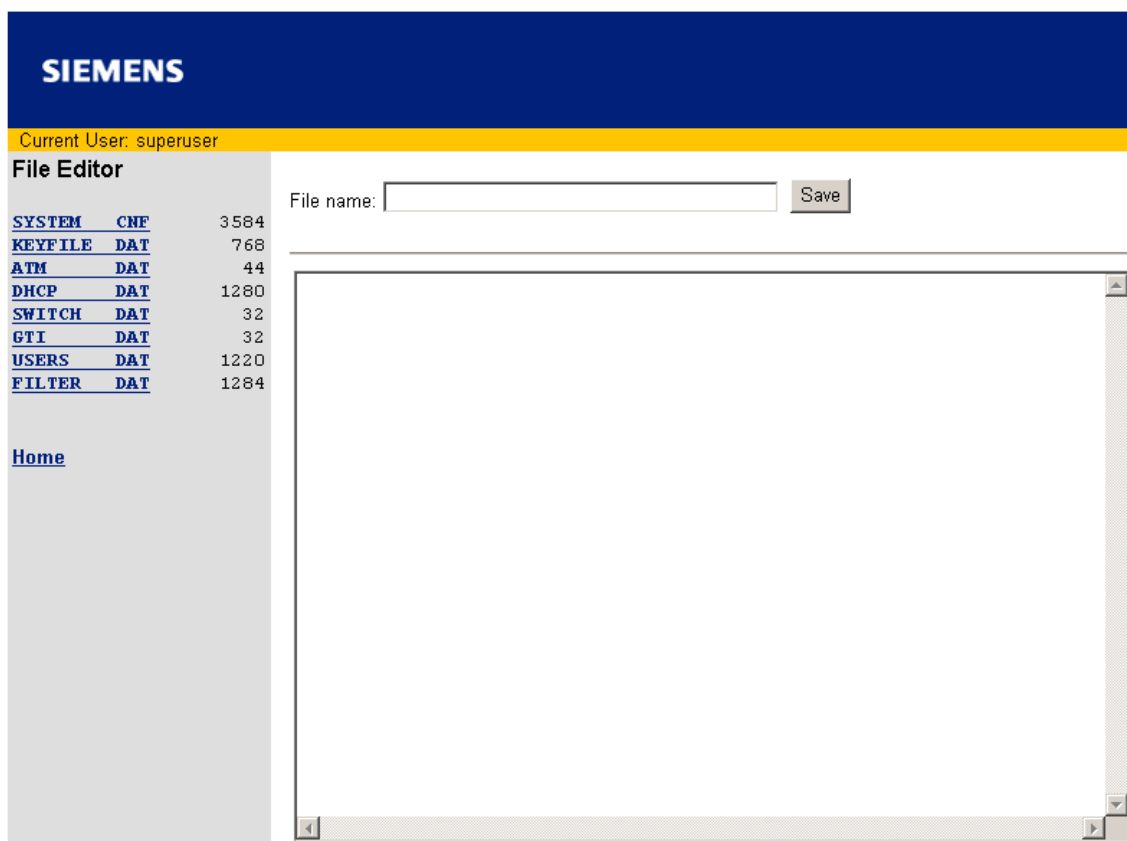
Volg de volgende stappen om een commando uit te voeren:

- Stap 1:** Voer uw CLI- commando in het betreffende veld in. Routeropdrachten moeten op precies dezelfde wijze worden ingevoerd als bij de prompt.
- Stap 2:** Klik op de knop Execute. Het Output Window toont alle output naar aanleiding van het commando.

File Editor

Het File Editor-scherm voorziet in een faciliteit voor het maken en wijzigen van bestanden die zijn opgeslagen op de router. Deze bestanden bevatten configuratiegegevens en andere data die door de router worden gebruikt. Gevorderde gebruikers kunnen het File Editor-scherm gebruiken om bestanden te openen, te wijzigen en vervolgens op te slaan. Voor gevorderde gebruikers die vertrouwd zijn met bestandsformaten en de syntax ervan is deze methode misschien efficiënter dan de configuratie van de router met behulp van commando's van de webinterface, vooral wanneer de hoeveelheid gegevens heel groot of complex is.

Scherf 67: File Editor-scherm



Om de File Editor te kunnen gebruiken, moet u de volgende stappen uitvoeren:

- Stap 1:** Kies het opgeslagen bestand dat u wilt gaan wijzigen uit de weergegeven lijst. De inhoud van het geselecteerde bestand is weergegeven in het bewerkingsscherm. U kunt ook een nieuw bestand maken door tekst in te voeren in het editorvenster.
- Stap 2:** Wijzig het bestand naar wens.
- Stap 3:** Voer een bestandsnaam in (filename.txt, max. 8 tekens voor de naam en 3 voor de extensie) in het venster File Name en klik op de knop Save. Uw bestand is opgeslagen onder de naam die u hebt opgegeven.

PAS OP! Als u een bestand met dezelfde naam op wilt slaan als die van een bestaand bestand, wordt het bestaande bestand overschreven.

U kunt alle wijzigingen ongedaan maken door te klikken op de knop Home onder aan het scherm.

IKE/IPSec Configuration

Internet Key Exchange/Internet Protocol Security (IKE/IPSec) is een veiligheidsfaciliteit voor de authenticatie en encryptie van IP-verkeer m.b.t. de authenticiteit, integriteit en privacy van uw verbindingen. IPSec-sessies komen tot stand via Security Associations (SA's) waarmee tussen veiligheidsapparatuur een bepaald niveau van veiligheidsattributen kan ontstaan dat nodig is voor een Virtual Private Network (VPN).

Het scherm voor de configuratie van IKE/IPSec toont de bestaande IKE- en IPSec-definities. Deze definities komen tot stand met behulp van de schermen Easy IKE/IPSec Setup en Advanced IKE/IPSec Setup.

Easy IKE/IPSec Setup

Het Easy IKE/IPSec Setup-scherm is hieronder te zien.

Scherf 68: Easy IKE/IPSec Setup-scherm

Efficient NETWORKS

Current User: superuser

Easy IKE/IPSec Setup

Internet Key Exchange (IKE) is a means of dynamically creating IP Security (IPSec) connections. IPSec uses encryption and authentication to create virtual private networks over an insecure network.

This screen will create a default IKE configuration.

The **IKE Peer Name** is a logical name for an IKE Peer. This name has no significance to the remote party.

The **Pre-shared Secret** is a mutually agreed-upon secret between both parties.

The **Peer Gateway IP Address** specifies the IP address of the other end of the IKE connection.

The **Destination IP Address** is the IP address of the remote private network that uses this policy.

The **Destination Subnet Mask** is the subnetwork mask of the remote private network that uses this policy.

[Advanced IKE/IPSec Setup](#)
[IPSec Main Page](#)
[Home](#)

Easy IKE/IPSec Setup

IKE Peer Name

Pre-shared Secret

Peer Gateway IP Address

Destination IP Address

Destination Subnet Mask

Om IKE/IPSec in te stellen met behulp van dit scherm, moet u de volgende stappen uitvoeren:

- Stap 1:** Voer een IKE Peer Name in het betreffende veld in. De naam is niet van belang voor een remote IKE peer. Kies een naam die u goed kunt onthouden.
- Stap 2:** Voer een Pre-Shared Secret in het betreffende veld in. Een Pre-Shared Secret is een case-sensitive teken dat wordt gebruikt voor de authenticatie. Deze Secret kan max. 256 tekens bevat-

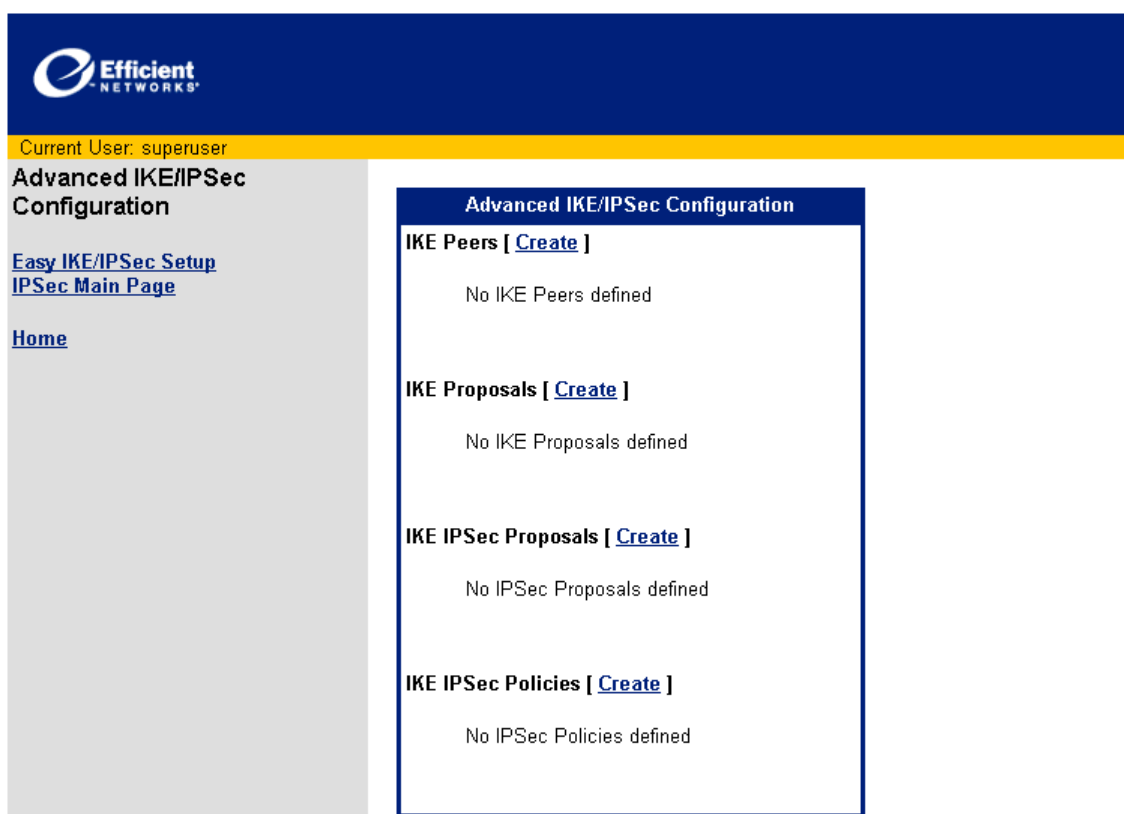
ten, zonder spaties en niet-afdrukbare tekens. De Pre-Shared Secret moet door allebei de zijden van een IKE-verbinding worden geaccepteerd.

- Stap 3:** Voer het IP-adres van de Peer Gateway in het IP Address Peer Gateway in. Dit IP-adres hoort bij de gateway van het remote einde van de IKE-verbinding.
- Stap 4:** Voer het Destination IP Address in het betreffende veld in. Dit is het IP-adres van het remote private netwerk dat uw router zal authenticeren met behulp van deze IKE Policy.
- Stap 5:** Voer de Destination Subnet Mask in het betreffende veld in. Dit is het subnetmasker van het remote privénetwerk dat uw router zal authenticeren met behulp van deze IKE Policy.
- Stap 6:** Klik op de knop Apply om uw nieuwe IKE/IPSec policy in te stellen en terug te keren naar het scherm Router Information.

Advanced IKE/IPSec Configuration

In het Advanced IKE/IPSec Configuration-schermbord staat informatie over uw IKE- en IPSec-peers, policy's en voorstellen. Elk deel van het scherm bevat een Create-link met andere schermen voor het activeren van nieuwe IKE- en IPSec-definities. Het Advanced IKE/IPSec Configuration-schermbord is hieronder te zien.

Schermbord 69: Advanced IKE/IPSec Configuration-schermbord



Dit Advanced IKE/IPSec Configuration-schermbord voorziet in de volgende soort informatie en links:

- **IKE Peers** - Hier staan alle gedefinieerde IKE Peers. IKE peers zijn die toestellen waarvan uw router weet dat ze deel kunnen nemen aan IKE-verbindingen. Klik op Create om nieuwe IKE peers te definiëren.
- **IKE Proposals** - Hier staan alle gedefinieerde IKE Proposals. IKE IPSec Proposals geven aan hoe pakketten worden authenticatieerd voor de laatste SA. Daarna bepalen IKE IPSec Policy's welke pakketten gecodeerd/geauthenticatieerd worden voor de afsluitende SA. Klik op Create om nieuwe IKE proposals te definiëren.
- **IKE IPSec Proposals** - Hier staan alle gedefinieerde IPSec Proposals. Klik op Create om nieuwe IPSec Proposals te definiëren.

- IKE IPSec Policies - Hier staan alle gedefinieerde IPSec Policy's. IPSec policy's zijn criteria voor datapakketten die door IPSec worden herkend, en acties die IPSec naar aanleiding van de herkenning zal starten. Klik op Create om nieuwe IPSec Policy's te definiëren.

IKE Peer Definition

Scherf 70: IKE Peer Definition-scherf

Efficient NETWORKS

Current User: superuser

IKE Peer Definition

NOTE: If the remote peer does not have a fixed IP address, enter "0.0.0.0" for the Peer Gateway IP Address and use Aggressive Mode.

The **IKE Peer Name** is a logical name for an IKE Peer. This name has no significance to the remote party.

The **Pre-shared Secret** is a mutually agreed-upon secret between both parties.

The **Peer Gateway IP Address** specifies the IP address of the other end of the IKE connection.

[Advanced IKE/IPSec Setup](#)
[IPSec Main Page](#)
[Home](#)

IKE Peer Definition

IKE Peer Name

Pre-shared Secret

Peer Gateway IP Address

Voer de volgende stappen uit om een IKE Peer Definition te configureren:

- Stap 1:** IKE Peer Name: Het eerste veld in het scherm IKE Peer Definition is voor het toekennen van een logische naam aan de IKE peer. De naam is niet van belang voor de remote IKE peer. Kies een naam die u goed kunt onthouden. Voer de IKE Peer Name in het betreffende veld in.
- Stap 2:** Pre-Shared Secret: Een Pre-Shared Secret is een case-sensitive teken dat wordt gebruikt voor de authenticatie. Deze Secret mag uit max. 255 tekens bestaan, zonder spaties of niet-afdruk-bare tekens. De Pre-Shared Secret moet door allebei de zijden van een IKE-verbinding worden geaccepteerd. Voer uw Pre-Shared Secret in het betreffende veld in.
- Stap 3:** Peer Gateway IP Address: Voer het IP-adres in van de gateway van het andere einde van de IKE-verbinding. Als de remote IKE peer geen vast IP-adres heeft, voer dan 0.0.0.0 in voor de Aggressive Mode in Phase 1 negotiations. Uw router ondersteunt twee fasen van 1 IKE-modi; Main en Aggressive. Uw router zal Main Mode gaan gebruiken als zowel het bron- als doel IP-adres bekend zijn. Uw router zal Aggressive Mode gaan gebruiken als hetzij het bron-IP-adres, hetzij het doel-IP-adres kan veranderen.
- Stap 4:** Klik op de knop Apply om uw nieuwe instellingen op te slaan en terug te keren naar het scherm Router Information.

IKE Proposal Definition

Scherma 71: IKE Proposal Definition-scherm

Efficient NETWORKS

Current User: superuser

IKE Phase I Proposal Definition

The **IKE Proposal Name** is a logical name for an IKE Proposal. This name has no significance to the remote party.

The **Message Authentication Scheme** is the hashing algorithm used to validate the IKE Phase I exchange.

The **Diffie-Hellman (Oakley) group** specifies the polynomial function for the IKE Phase I exchange.

The **Encryption Type** specifies the encryption algorithm that will be used during the IKE Phase II ("Quick Mode") exchange.

The **Phase I Proposal Lifetime** is the duration of time after which the Phase I negotiation expires. A new IKE Phase I exchange will occur automatically.

[Advanced IKE/IPSec Setup](#)
[IPSec Main Page](#)
[Home](#)

IKE Phase I Proposal Definition

IKE Proposal Name

Message Authentication Scheme

Diffie-Hellman (Oakley) group


Encryption Type

Phase I Proposal Lifetime (seconds)

- Stap 1:** IKE Proposal Name: Voer een logische naam in voor de IKE Proposal Definition. De naam is niet van belang voor de remote IKE peer.
- Stap 2:** Message Authentication Scheme: Kies een van de twee message authentication schemes:
- MD5: Voorziet in authenticatie van meldingen d.m.v. Message Digest 5.
 - SHA1: Voorziet in authenticatie van meldingen d.m.v. Secure Hashing Algorithm 1 (standaard).
- Stap 3:** Diffie-Hellman (Oakley) Group: Kies de Diffie-Hellman key generation group uit de twee Diffie-Hellman group-opties:
- Group 1: Pas Diffie-Hellman Group 1 (768 bits) toe.
 - Group 2: Pas Diffie-Hellman Group 2 (1024 bits) toe.
- Stap 4:** Encryptietype: Bepaal het type encryptie dat u wilt voorstellen:
- DES: Encrypt using a 56-bit key.
 - 3DES: Encrypt using three 56-bit keys to produce 168-bit encryption.
- Stap 5:** Phase 1 Proposal Lifetime: Bepaal de duur van dit voorstel, gemeten in seconden. De standaardinstelling is 86400 seconden (24 uren). Zodra deze lifetime is verstreken, zal uw router de IKE-verbinding opnieuw tot stand brengen.
- Stap 6:** Klik op de knop Apply om uw nieuwe instellingen op te slaan en terug te keren naar het scherm Router Information.

IKE IPSec Proposal Definition

Scherf 72: IKE IPSec Proposal Definition-scherf



Current User: superuser

IKE IPSec Proposal Definition

The **IPSec Proposal Name** is a logical name for an IPSec Proposal. This name has no significance to the remote party.

The **AH Authentication Scheme** is the hashing algorithm used for Authentication Header (AH) IPSec.

The **ESP Authentication Scheme** is the hashing algorithm used for Encapsulating Security Payload (ESP) IPSec.

The **ESP Encryption Scheme** is the algorithm used to encrypt ESP IPSec packets.

The **IP Compression Method** is the algorithm used to compress IPSec packets.

The **Phase II Proposal Lifetime** is the duration of time after which the IKE Phase II negotiation expires. A new IKE Phase II exchange will occur automatically.

The **Phase II Proposal Lifedata** is the number of kilobytes of data after which the IKE Phase II negotiation expires. A new IKE Phase II exchange will occur automatically.

[Advanced IKE/IPSec Setup](#)
[IPSec Main Page](#)
[Home](#)

IKE IPSec Proposal Definition

IPSec Proposal Name

AH Authentication Scheme

ESP Authentication Scheme

ESP Encryption Scheme

IP Compression Method

Phase II Proposal Lifetime (seconds)

Phase II Proposal Lifedata (KBytes)

- Step 1:** IKE IPSec Proposal Name: Voer een logische naam in voor de IKE IPSec Proposal Definition. De naam is niet van belang voor de remote IKE IPSec peer.
- Step 2:** AH Authentication Scheme: Welke AH-methode wilt u voorstellen:
- Opmerking: Request no AH encapsulation.
 - MD5: Request AH encapsulation and authenticate using Message Digest 5.
 - SHA1: Voorziet in authenticatie van meldingen d.m.v. Secure Hashing Algorithm 1.
- Step 3:** ESP Authentication Scheme: Kies een ESP message authentication uit als voorstel:
- Opmerking: Voorziet niet in authenticatie van meldingen.
 - MD5: Voorziet in authenticatie van meldingen d.m.v. Message Digest 5.
 - SHA1: Voorziet in authenticatie van meldingen d.m.v. Secure Hashing Algorithm 1.
- Step 4:** ESP Encryption Scheme: Bepaal de encryptiemethode (mits beschikbaar) die u wilt voorstellen:
- DES: Use ESP encapsulation and 56-bit encryption.
 - 3DES: Use ESP encapsulation and three 56-bit keys to produce 168-bit encryption.

- NULL: Deze optie voorziet in ESP encapsulation, maar niet in data encryptie. Met behulp van de ESP encapsulation kan de bron worden geverifieerd, maar de data worden ongecodeerd verzonden ten behoeve van een betere throughput.
- Opmerking: Deze optie maakt geen gebruik van ESP encapsulation en evenmin van encryptie.

Stap 5: IP Compression Method: Kies om te bepalen of u LZS IP compression wilt voorstellen of geen IP compression.


Stap 6: Phase II Proposal Lifetime: Voer de tijdsduur in (in seconden) voor de IPSec SA afloopt. De standaardinstelling is 1800 seconden. Zodra deze lifetime is verstreken, zal uw router de IKE-verbinding opnieuw tot stand brengen.

Stap 7: Phase II Proposal Life Data: Voer de hoeveelheid data in (in KB) voor de IPSec SA verstrijkt. Nadat de gewenste hoeveelheid data is overgedragen, zal uw router de IKE-verbinding herzien. Kiest u voor 0 (zero), dan is de hoeveelheid data onbeperkt. Door de hoeveelheid data die overgedragen moet worden, te beperken, kunt u het gevaar indammen dat een key wordt gestoord.

Stap 8: Klik op de knop Apply om uw IKE IPSec Proposal Definition op te slaan en terug te keren naar het Home-scherm.

IKE IPSec Policy Definition

Scherf 73: IKE IPSec Policy Definition-scherf



Current User: superuser

IKE IPSec Policy Definition

The **IPSec Policy Name** is a logical name for an IPSec Policy. This name has no significance to the remote party.

The **Peer Binding** identifies the remote peer for which this policy applies.

The **PFS Group** identifies the Diffie-Hellman group for Perfect Forward Secrecy.

The **IPSec Proposal Bindings** identify the IPSec Proposals which may be used for this policy.

The **IP Protocol** identifies the protocol of the IP traffic that uses this policy.

The **Source IP Address** is the IP address from the local private network that uses this policy.

The **Source Subnet Mask** is the subnetwork mask of the local private network that uses this policy.

The **Destination IP Address** is the IP address of the remote private network that uses this policy.

The **Destination Subnet Mask** is the subnetwork mask of the remote private network that uses this policy.

The **Source Port** is the source port of the TCP/UDP traffic that uses this policy.

IKE IPSec Policy Definition

IPSec Policy Name

Peer Binding

IPSec Proposal Bindings

PFS Group

IP Protocol

Source IP Address

Source Subnet Mask

Destination IP Address

Destination Subnet Mask

Source Port

Destination Port

- Stap 1:** IPSec Policy Name: Voer een logische naam in voor de IPSec policy. De naam die u kiest, is niet van belang voor de andere zijde van IPSec. Kies een naam die u goed kunt onthouden.
- Stap 2:** Peer Binding: Geef de remote IKE peer aan op welke de policy toegepast moet worden. Deze Peer moet al zijn gedefinieerd met behulp van het IKE Peer Definition-scherf.
- Stap 3:** IPSec Proposal Bindings: Bepaal een IKE IPSec proposal die u samen met deze policy wilt gebruiken. De IKE IPSec-voorstellen moeten al zijn gedefinieerd met behulp van het IKE IPSec Proposal Definition-scherf.
- Stap 4:** PFS Group: Bepaal de Perfect Forward Secrecy negotiation en Diffie-Hellman group die u voor de rekeys wilt gebruiken. Perfect Forward Secrecy zorgt dat de key exchange nog veiliger is. Als een key wordt gestoord, zullen alleen de data die door deze key werden beschermd, eveneens makkelijk aangetast kunnen worden. U kunt kiezen tussen None, Group 1 of Group 2.
- Stap 5:** IP Protocol: Geef een protocol aan dat u samen met deze policy wilt gebruiken. Ook kunt u elk gewenst protocol gebruiken door All te selecteren.
- Stap 6:** Source IP Address: Voer het IP-adres in van het LAN dat gebruik maakt van deze policy. Dit is meestal het IP-adres dat is toegewezen aan het netwerk lokaal op uw router.

- Stap 7:** Source Subnet Mask: Voer het subnetmasker van het LAN in dat gebruik zal gaan maken van deze policy. Dit is meestal het subnetmasker dat is toegewezen aan het netwerk lokaal op uw router.
- Stap 8:** Destination IP Address: Voer het IP-adres van het andere privénetwerk in waarmee u router de verbinding via deze policy tot stand zal brengen.
- Stap 9:** Destination Subnet Mask: Voer het subnetmasker in van het andere privénetwerk waarmee uw router een verbinding via deze policy tot stand zal brengen.
- Stap 10:** Source Port: Voer de poort in dat de bron zal zijn van het TCP/UDP-verkeer onder deze policy. U kunt All ports, een poortnummer of een IP-toepassing in verbinding met een bepaalde poort opgeven.
- Stap 11:** Destination Port: Voer de poort in dat het doel zal zijn van het TCP/UDP-verkeer onder deze policy. U kunt All ports, een poortnummer of een IP-toepassing in verbinding met een bepaalde poort opgeven.
- Stap 12:** Klik op de knop Apply om uw IKE IPSec policy te activeren en terug te keren naar het scherm Router Information.

Voorzijde

Scherf 74: Aanzicht voorzijde



Table 1: LED's aan de voorzijde

LED	Kleur	Beschrijving
Power	Groen Uit:	Power is AAN Power is UIT
Test	Geel: Geel, knipperend: Groen (2 sec. knipperen): Uit:	POST POST is uit POST gelukt Router is geannuleerd
WANT	Groen, knipperend: Groen:	WAN-transmissies ontdekt Geen WAN-transmissies ontdekt
WANR	Groen, knipperend: Groen:	WAN-ontvangst ontdekt Geen WAN-ontvangst ontdekt
LANT	Groen, knipperend: Groen:	LAN-transmissies vastgesteld Geen LAN-transmissies vastgesteld
LANR	Groen, knipperend: Groen:	LAN-ontvangst ontdekt Geen LAN-transmissies vastgesteld

Achterzijde

Scherf 75: Aanzicht achterzijde

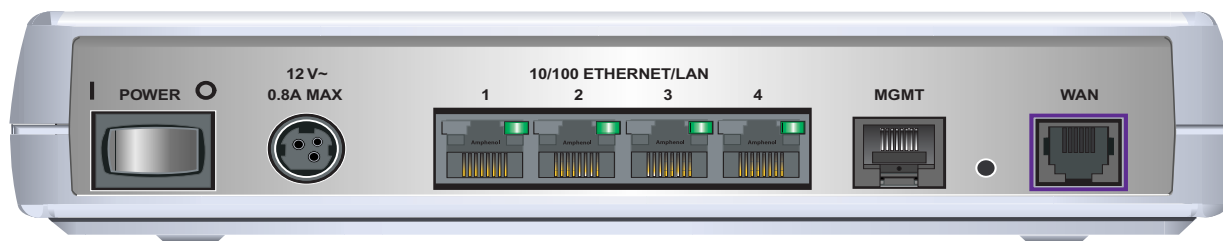


Table 2: 5830 Router achterzijde

Verbinding	Functie
Power	Maakt gebruik van een 12V AC/DC-netadapter.
Ethernetpoorten	Vier Ethernet T-100 switched ports (8-pins, RJ-45)
Managementpoort	Deze 8-pins, RJ-45-poort voorziet in een RS232-aansluiting voor console-verbindingen.
DSL/WAN Port	Een 8-pin RJ-45-poort zorgt voor de verbinding met DSL.

Hardwarespecificatie

Fysieke specificatie

- Afmeting: (b x d x h) 13,25 x 9,5 x 1,8 inches
- (b x d x h) 33,66 x 24,13 x 4,6 cm
- Gewicht 680 g.
- .68 Kg.

Operationele omgeving

- Temperatuur: 40F tot 105F, 5 tot 40C
- Luchtvochtigheid: 20% tot 80%; geen condensvorming

Voedingseisen

- AC voltage: 100 tot 120V AC of 220 tot 240V AC
- Frequentie: 50/60 Hz
- Verbruik: 10 W max.
- Ingebouwde stroomvoorzorging met aan-/uitschakelaar

Processor

- Motorola 64 MHz MPC857DSL
- 8MB SDRAM, 4MB flash memory
- DES, 3DES, MD5, SHA hardware assist
- Externe Real Time Clock (RTC)-chip met noodstroomvoorziening (batterij)

LAN Interface

- Ingebouwde achtpoortige Ethernet-schakelaar met RJ-45-stekkers.
- Groene/amber LED
- LAN-snelheid van 10 of 100 Mbps, vol of half duplex, met auto-senseschakelaar

WAN Interface

- Een DSL-interface:
- ADSL, Annex A
- RJ-45 met 4-5 pinout (center pair)

Seriële interface

- Een RS-232 asynchrone console of externe modempoot (RJ-45)

Keuringseisen

- CE-label
- TUV
- Veiligheid: UL 1950, CSA 22.2, EN 60950
- Straling: FCC Part 15 Class B, EN55022
- Weerstand: EN50082-1, EN55024

Softwarespecificatie

Bridging

- Transparent bridging inclusief Spanning Tree-protocol (IEEE 802.1D)
- Bridge filters

Routing

- TCP/IP met RIP1 (RFC 1058), RIP1 compatibel en RIP2 (RFC 1389) of statische routing binnen het LAN of WAN
- Novell IPX met RIP/SAP (RFC 1552)
- DHCP-client (RFC 2132)
- DHCP server - Automatische toekenning van IP-adressen, subnetmasker, standaard gateway- en DNS serveradressen aan DHCP-clients (RFC 2131, 2132)
- DHCP relay agent
- DNS relay
- Multiple subnets on LAN
- Virtual routing
- Virtual Router Redundancy Protocol (RFC 2338)

Configuratiemanagement

- Easy Setup Web Management Interface
- Microsoft Windows-configuratiemanagement via SNMP
- TFTP download/upload van nieuwe software en configuratiebestanden
- Performance monitor
- Dynamische logging van events en history
- Beheer via HTTP, SNMP, Telnet of VT100-terminal
- Een netwerkstart maakt gebruik van de BootP-server (RFC 2131, RFC 2132)

Diverse diensten - Quality of Service Provisioning

- Weighted Fair Queuing (WFQ)

- Differentiated Services (DiffServ)

Dial Backup

- Failover naar modem via consolepoort
- Web Management Interface
- User selectable fail/restore criteria
- Optionele modemstekker (DB9 of DB25)
- Ondersteund L2TP en IPSec tunnel failover

Asynchronous Transfer Mode (ATM)

- Encapsulation (IP, Bridging and Bridge Encapsulated Routing) (RFC 1483)
- PPP via ATM (LLC en VC multiplexing) (RFC 2364)
- PPP via Ethernet
- Klassieke IP (RFC 1577)
- AAL5 voor data
- Multiple Virtual Circuits (VCs)
- L610 OAM F5 loopback

IP Address Translation

- Network renumbering (RFC 1631)
- Network Address Translation (NAT)
- LAN-servers die door NAT worden ondersteund
- Support voor NAT binnen een IPSec-tunnel

Protocol-conformiteitstest

- RFC 1483 (Bay Networks™, Cabletron™, Cisco™, Redback™)
- PPP via ATM (Cisco, Escalate™, Redback) (RFC 2364)

PPP (RFC 1661)

- Datacompressie tot 4:1 (STAC™ LZS) (RFC 1974)
- Van Jacobsen header compression (RFC 1144)
- Spoofing en filtering (IP-RIP, IPX-RIP, SAP, Watchdog, serialization)
- Automatische IP en DNS-toekenning (RFC 1877)
- PPP via Ethernet (RFC 2516)

Veiligheid

- Role-based management
- Gebruikersauthenticatie (PAP/CHAP) met PPP (RFC 1334, RFC 1994)
- Wachtwoordcontrole ten behoeve van de Configuration Manager
- SNMP password and community name reassignment
- HTTP/Syslog/SNMP/Telnet port reassignment, access control list
- VPN support (L2TP, IPSec, IKE, DES, 3DES)
- Firewall (IP filtering)
- Stateful Firewall (ICSA compliant)
- Secure Management Communications - IPSec en SSH
- 3DES hardware assist
- Radius-serversupport
- VPN Hardware Acceleration support

Neem voor specifieke productsupport contact op met het bedrijf of de instantie waarvan u de apparatuur hebt gekocht. Als u contact moet opnemen met uw netwerkprovider voor technische ondersteuning, zorg dan dat u de volgende informatie bij de hand hebt:

- Modelnummer van de router (aan de onderzijde van het toestel)
- Softwareversie van de router (weergegeven in de Command Line and Web User Interface)
- Datum van aankoop
- Besturingssysteem (bijv. Windows 95, 98, 2000, NT, XP, MacOS, Linux of Unix)
- Een gedetailleerde beschrijving van het probleem